MARRAKECH – At-Large Capacity Building Session: Current issues in Cybersecurity
Wednesday, June 26, 2019 – 12:15 to 13:15 WET
ICANN65 | Marrakech, Morocco

JOANNA KULESZA: So, hello everyone. Good afternoon. Thank you for joining us. My name is Joanna Kulesza. I'm on the ALAC. I'm a EURALO individual member. And I'm also co-chairing the Capacity Building Working Group of the At-Large Community, together with Alfredo Calderon, who could, unfortunately, not join us here in Marrakech.

I welcome the At-Large members, but I also welcome members of other communities and constituencies. We are considering this workshop as a part of a joint collaboration with the GAC, in terms of capacity building, so I hope there are some GAC members who have managed to find the time to join us here today. And I welcome all members of other constituencies that I see represented here in the room.

Now, the topic of our presentation today is the Current Issues in Cybersecurity. As I have mentioned previously today, during the GAC session, At-Large attempts to prioritize both security and privacy –the work that is being done the EPDP-wise and on the privacy aspect. And the work we're trying to do here is to provide a better understanding of current issues in cybersecurity.

A part of that endeavor has been a series of webinars we have conducted for participants of the ATLAS III conference, that's coming up later this year in Montreal. That was, as already mentioned, a series of five webinars, that provided updates and multilingual information to the potential participants of ATLAS III, but the webinars were open to anyone wishing to participate. They are still available online. If you wish to look them up, just let us know. We'll be happy to guide you.

One of the webinars that provoked particular interest, and enjoyed great attention from the community, was one similar to that, that Patrick is going to present today. It also covered current issues of cybersecurity. We particularly appreciated Patrick's input, because it covered both the technical aspects and the policy aspects, so to speak.

Now, our guest today is Patrick Jones, who works with the Global Stakeholder Engagement team here at ICANN. I appreciate Patrick's angle, because myself, I'm also not a technical expert, and Patrick has a rich engagement with civil society, government, all the groups that are represented in this multi-stakeholder model.

In that context, I am really, really looking forward to your presentation, Patrick. Thank you for taking the time to join us. And let me take this opportunity to thank you, also, for the

webinar. All the materials will be available. They are available on the ICANN Wiki. We will be posting the links on Twitter. They are available, also, in the agenda.

We have just an hour for this session. Patrick has assured me that he will allow plenty of time for discussion and questions. We are particularly looking into that. Keep in mind, this is a capacity building session. So, what we want you to take away is a better understanding of the current issues. And this can also be used as a platform for us to try and think about our approach to cybersecurity. What does that mean in the ICANN context? I think everyone has easily settled in with their lunch, so that gives me a wonderful opportunity to hand the floor over to Patrick. Once again, thank you for joining us. Patrick, the floor is yours.

PATRICK JONES: Thank you, Joanna, and thank you very much for having me speak, once again, to the At-Large and the wider community. This is somewhat of an update from the webinar that David Huberman and I delivered. It feels like several months ago, but I guess it was last month. And this talk makes use of some new information. There's new material that comes out all the time. There's always a new threat—an attack that happens. So, what you will see are some of the latest updates that we've put into our material from the recent DNS Symposium in Bangkok, as well as some other

ICANN announcements that you may have seen through our Twitter handle in the past few weeks. Next slide.

A bit about myself. I am with our Global Stakeholder Engagement Team, but I've been at ICANN over 13 years. I've had a number of roles, including about five years with our ICANN Security Team. And I do quite a bit of DNS technical trainings with various communities. Within the past two weeks, I was in Latvia and Lithuania, and also Poland. And again, I work very closely with our Office of the CTO team.

I'm going to start today by introducing some examples. Unfortunately, the resolution of the aspect of the slides is a little large. But what you can see is that every week, you may see some headlines about attacks that occur. This particular one is from 2017, about the Mirai Botnet, which was a domain-generating algorithm that leveraged web cameras from around the world. And at the time, it was the largest distributed denial of service attack platform. It was actually created in 2016 by three college students. And the purpose for their botnet was to take out servers that were associated with the popular computer game, Minecraft.

This attack, and a series of attacks associated with the botnet, had a collateral effect on cloud systems that hosted hundreds of domains around the world. There was a statistic from March of 2019 that an hour of downtime from a denial of service attack

costs approximately $222,000 per hour. When you think about it, these figures add up significantly around the world for businesses and users. Next slide.

This was this week, heading into Marrakech. And people may have heard about, NASA was hacked. Someone had plugged in a Raspberry Pi unit into their servers—into their systems—and they were able to move laterally throughout the NASA network and acquire sensitive data about ongoing and upcoming missions. This happens all the time. And this isn't within an ICANN context, but it's just an example for you that this has major impacts for governments, for universities, researchers, and others.

Here's another example … next series of headlines from February of this year, describing a series of DNS-related attacks that hit a number of registries, hosting providers—even Packet Clearing House and Netnod, which are some major platforms. Those organizations have talked very frankly about the attacks that hit them, at the DNS Symposium in Thailand. Packet Clearing House described on the attack on their systems, what they did to recover, what they did to acknowledge those attacks.

If we go to the next slide, this is another headline that even mentions ICANN. And you may have read our announcement from mid-February that came from the ICANN CTO team, describing the types of threats—more collecting of the links from

other organizations—and warning the global internet community about these types of threats. So, I'll have more information about that coming up. Next slide.

So again, this is another recent example. While I was in Europe, ICANN sent out this tweet with a blog post that described, "Beware of phishing," and what you could do, steps you can take to recognize that this is happening. ICANN puts out announcements and links such as this. We want to try to raise the awareness for the community, that these types of things happen. We can go to the next slide.

So, one of the reasons why this is occurring is if you think about how much trust we put in the internet. We're approaching anywhere from 30 to 50 billion devices that are connected to the Domain Name System. And all of these devices, they generate and transmit data between machines, between jurisdictions, and those are attractive targets for attack.

Again, in the next slide, you can see that a key message that you should consider is that your data between machines and devices does provide an attractive target. The Security and Stability Advisory Committee recently published their latest document. It's called SAC105, and it provides … It's more of a tutorial-style document, and it's describing the connection between the internet of things and the DNS. And so, if you haven't read that

document, I really encourage you to do so. There will be a session at this meeting, that's open to the community, about that document. And SSAC members will be providing an update to the community. I know they often come to At-Large, so you'll be interested in asking them about that document.

So, when you think about the common elements that are found in a company's network, or a university's network, or inside a government network, or a business, they all these types of things. So, every business and organization, they have email. They have calendaring. They have contacts. Those are hosted on mail servers. They'll have databases, that either have their customer data or their employee data. That includes everything from their tax information … There's just substantial data that organizations hold on their customers and others. And they also have file systems and financial information. They have trade secrets, and their organizational processes and procedures.

So, when you think about what underpins those elements—the next slide—it includes everything from key management … So, it's usernames, passwords, biometrics. You might utilize multifactor authentication. You may have some kind of data storage and data retention practices. You may have governance and other structure to support those systems and documents. And if you are an organization, you also rely on the DNS to have a web presence and connect out to other systems. So, every day,

those elements and systems are under attack, and attackers are trying to penetrate those systems, extract data, and exploit any vulnerabilities they can to get to that information. Next slide.

Now, in an ICANN context, I want to provide some definitions of what we mean in the terms that we're using, just to level set here. When we're talking about phishing, we're talking about the practice of sending email. It pretends to be from a trusted organization, and it's trying to trick the user to reveal some type of personal information, whether it's passwords, or credit cards, or banking information—other financial details that these attackers can then exploit.

Malware is software that is designed to, again, disrupt networks—perhaps damage those networks or gain unauthorized access to a computer system. You might be familiar with some of the headlines about hospital systems in major cities – City of Baltimore, there was another city in Florida, in the United States – that were hit with ransomware. And then, these cities, hospitals, and other organizations have to make the decision. Do we pay the ransom to get our passwords back?

The next term, a botnet … So, it's a robot network—a network of computers and machines. They can also be web cameras or other internet of thing devices that are then infected with some type of software, and they can be controlled as a group, either without

the owner's knowledge or as a large-scale platform that can then be rented out to malicious actors.

There's quite a bit of discussion at ICANN about what we mean by DNS abuse. Currently, there's no globally accepted definition. There's much discussion about this within the GAC's Public Safety Working Group and in other sectors of ICANN. But generally, what we're talking about are things related to cybercrime, whether it's some time of malicious conduct, hacking. We tend to see the threats to the Domain Name System that fall into the categories of privacy violations, denial of service attacks, and data corruption. The point is that these attackers are trying to exploit the Domain Name System so that they can trick, defraud, and deceive users. Next slide.

Going to add a little bit more nuance to this. Our Office of the CTO team regularly talks about DNS abuse, and we try to distinguish between … DNS abuse is anything that refers to attacking or using the DNS infrastructure for some purpose, versus misuse, which often is exploiting the protocols and the Domain Name Registration processes for some type of malicious purpose. Next slide.

Now, I took this slide from a presentation that was given just last week by our new ICANN Board Liaison from the SSAC. This is from Merike Kaeo. She tried to distinguish between the different types

of DNS abuse that we see. So, we see everything from attacks on the protocols and the servers, and they're described here. You can find these slides on the At-Large session notes, so I won't spend a lot of time going into each one of these. But it's helpful to try to talk about the different types of attacks that we're seeing. If you go to the next slide …

What's ICANN's role in this? Sometimes, our role is quite limited, but we do serve as a connection point for different organizations and communities. These types of attacks often involve governments, multinational corporations, and global law enforcement, and are quite prominently featured in the news. So, at this meeting—in fact, this morning—we had some discussions between the GAC's Public Safety Working Group and SSAC members, and I'm sure those groups will be talking to other parts of the community. There is a role for community and ICANN Org that is before, during, and after these types of incidents occur. Next slide.

At the ICANN meeting in Kobe, SSAC members presented about the recent domain registration hijacking attacks that have been occurring since late last year. I'm going to provide a bit more context. Some of this is repeating information that was presented by SSAC, but there's also some new information in this, too. Next slide.

In the attacks that have been occurring and ongoing … These have been labeled as DNS espionage or the Sea Turtle types of attacks. The research that's underway has been trying to … Doing attribution is hard, and ICANN takes no position whatsoever on who is behind these types of attacks. You may see other organizations identifying the attacks as done by a particular state actor. We're not going to say one way or the other.

But these are examples of what's been referred to as cyber offense prepositioning. So, it's the gathering of intelligence that might be used to later launch a well-organized cyberattack. In the attacks that occurred, they started out primarily impacting organizations, airlines, banks, ministries in countries throughout North Africa and the Middle East. So, it's important for this region to understand that this is where some of these attacks were occurring.

These attacks started out going after registries, and registrars, and large providers. So, I mentioned Netnod and Packet Clearing House were two large organizations that were also impacted. I believe there some ccTLDs that were impacted in this. Armenia's been mentioned as one. Next slide.

So, this gives you a visualization of where these events occurred. During the attacks, the parties involved had the ability to modify registration records at the registry. They did this through

compromising login credentials. The attackers also changed the name servers and pointed the zones for these name servers to the attackers' DNS servers. And there was also modification of the A records and the mail server records associated with these domains. And then once the zones were redirected, the attackers could then impersonate servers—but the service is hosted by the victims—and extract further information.

Now, this information was presented at the Kobe meeting. First, the attack was identified by Cisco's Talos Security Team. They thought that this was an ongoing campaign that was targeting Lebanon and other domains and businesses in the United Arab Emirates. And then, there was another report from a company called FireEye in January of this year. And then, shortly after that, there were other announcements that were released. Netnod released their statement in February. They also presented on this topic at their Netnod spring meeting. And then, there were sessions at the ICANN meeting in Kobe from SSAC about this.

Next, we'll go into a little discussion about ICANN's role before these types of incidents occur. So, next slide. It's in our bylaws that we put a strong emphasis on ensuring the secure and stable operation of the unique identifiers systems for the internet. And we also have the commitment to preserve and enhance the administration of the DNS. We have a function within ICANN, Office of the CTO team, that does regular training, engagement,

and outreach with the technical community. But it's not only with those communities. There's other communities that are impacted. Next slide.

In our revised strategic plan—actually, this is now approved by the board—security has a prominent focus. The first objective, for our next five years, are going be about strengthening the security of the DNS and the DNS root server system, and also evolving the unique identifier systems to coordinate a collaborate with the relevant parties. Next slide.

Throughout our meetings here, there are a number of groups that are working on security, stability, and resiliency issues. So, I mentioned the GAC's Public Safety Working Group. This group focuses on aspects of ICANN policies and procedures that are related to DNS abuse and cybercrime mitigation. It's ongoing discussions that are happening this week. We have Security and Stability Advisory Committee, that also works on ongoing threat assessment and risk analysis, presenting papers and writing documents that are, while aimed at the ICANN Board, are also aimed at the wider ICANN community. And then, we also have the Root Server System Advisory Committee, that advises the board and the community on matters that relate to the root server system.

You've probably seen – or if you haven't seen yet, you should definitely take a look at – the public comment that is on the potential evolution of the root server system. I would think that At-Large would be very interested in that document, and that's currently out for public comment. Next slide.

Now, hopefully this will help put into context that there are quite a bit of relationships between the parties that are governed by contracts. We have the agreement between ICANN and the generic, top-level domain registry operators. Those registries also have agreements between themselves and their registrars that offer those domains that they manage. ICANN has a registrar accreditation agreement with all accredited registrars. And those registrars may have resellers, so they have an agreement between themselves and the reseller.

The reseller and the registrar may also have—and certainly do have—an agreement between themselves and the registrant. ICANN doesn't have a direct contractual relationship between the registrants that register these names. But this hopefully will help show the chain of connection between the different parties.

Now, in our contracts, there are some important tools that are related to security and stability, that the current registrar accreditation agreement imposes a duty to investigate abuse. The latest registry agreements also have similar abuse provisions,

including that the registry operator will prohibit registered name holders from distributing malware, abusively operating botnets, conducting phishing, doing piracy, trademark/copyright infringement, fraudulent and deceptive practices, counterfeiting, or otherwise engaging in activity that's contrary to the law.

So, at ICANN, we also have our subsidiary Public Technical Identifiers. This is responsible for the operational aspects of allocating member resources to the regional internet registries. We also maintain the root zone for the DNS, administer the dot ARPA zone, and we're responsible for managing the trust anchor for domain name security extensions, which takes us into the next slide.

A little bit about what this is … I'm not going to spend a lot of time going into detail on it, but hopefully you understand that when the DNS was developed by engineers in the mid-1980s, security was not built into the protocols. So, DNSSEC was developed, particularly after some research that identified that users and visitors to domains could be misdirected.

So, DNSSEC is attempting to provide some assurance to registrants, that the information they're seeing when they go to page is the page that they're intending to go to. This allows registrants to sign their data, but also allows operators to validate that the information that they're passing along is from their

organization. So, if you're in a browser that is DNSSEC enabled, you may see a green key or a lock. It gives you some assurance that if you're going to a domain that's signed, that it's actually the domain you're intending to go to.

So, when there is an incident that's occurring, it's helpful to understand that ICANN has a team that is primarily the main point of contact for different organizations. We try to coordinate responses with those organizations. This group has a long history of coordinating with different actors and different parties, and working closely with trusted communities. And they use their deep understanding and their expertise to help connect different groups together.

So, when this is occurring, these types of attacks need to be coordinated. ICANN is a member of the Forum for Incident Response Security Teams. And so, that's the collection of computer emergency response teams, other security professionals, that work to share information together. There's also the TLD-OPS list at ICANN, which is started from—and it's primarily country code operators. They can share information with each other when there is an attack that's happening.

So, ICANN Org, staff, and community, we regularly participate together in efforts to teach other organizations about issues impacting the DNS and the unique identifier system. We do this

through webinars, how-it-works sessions at ICANN meetings. We do this through technical workshops, such as the DNS Symposium, and also with global law enforcement trainings. So, this is an example of one that just occurred earlier this year, in this region. And it's an effort to share information and best practices, raise awareness of issues, and really bring this information to the regions.

In this particular example, some members from our team worked closely with the Pakistan Telecommunication Authority to do a multi-day workshop on capacity development—improving of skills and raising awareness of particular issues with the telco sector and other stakeholders. Often, these sessions are open, and businesses can attend. I did two within the last few weeks, and that included members from academic community, [cert] teams. There were some local law enforcement, ccTLD managers, and other organizations who have been part of these trainings. We also deliver these as webinars, too.

Now, this is taken from the talk that I gave at Tech Day, earlier this week. We often do DNSSEC trainings in the regions. We do this to, one, raise the awareness of domain name security issues, but also take it down to a level that can be understood by regulators, and decision makers, and businesses. Sometimes, we do more hands-on training. And we have a train-the-trainer program where those in the regions can then take this information, and go out, and

deliver the training. ICANN can't go everywhere, so this is actually quite useful to train community partners to deliver this information.

And we do this to help spread the message and build the chain of trust in the domain name system. So, we want to encourage all TLD managers to implement DNSSEC. We want to encourage ISPs to turn on validation and raise the awareness that they should be following good practices. Some current statistics … So as of at least two days ago, there were approximately 1,398 top-level domains that were signed with DNSSEC, and that's out of the total of 1,530 TLDs in the root. About 50 percent of the country code TLDs are signed, and there's quite a bit of demand around the world for this DNSSEC deployment expertise.

So, it's hard to draw a straight line from the delivery of the training to showing a country code manager, or an operator, that decide to sign their zones. But we are seeing an increase, particularly recently, in a number of TLDs that are turning on DNSSEC, particularly in the last three months. And so, I think that does show that by delivering the training, that people then go out and implement.

And I think the Kuwait example is a particularly really good one, because the ccTLD manager for Kuwait attend the train-the-trainer session that I helped deliver in Turkey last year. And they

went back, and then implemented it on their own. And in fact, the Kuwait ccTLD was part of the training delegation in Pakistan that's helping to get them signed. So, that's showing where we've gone and delivered a training, people take on those skills, and implement.

So, within FY19, we've gone to a variety of places. Just for your awareness, that we do a variety of training. The local community trainings cover a variety of topics, from DNS fundamentals and understanding the DNS ecosystem, to understanding abuse. We also try to touch on issues related to general top-level domains, internationalized domain names, universal acceptance. And we've tried to work in current topics, like emoji domain issues, as well as recent guidance on the DNS attacks. So, you can see that this includes trainings that we've done at network operator group meetings, regional TLD organization meetings, and others.

So, again, it's hard to always show the impact of these hands-on trainings, but over time, I think this is a good example of where, by going and doing this direct outreach, we are showing a benefit. So, I'll go back about 10 years. We've had a quite a bit of community collaboration around the Conficker Botnet, and then other botnets since then, the Avalanche and Andromeda domain-generating algorithm botnets. We've also had registries that have implemented and used an expedited registry security request

system. So, this gives them a contractual waiver from ICANN on actions that they take to mitigate malicious conduct.

ICANN has a coordinated vulnerability disclosure process, and everyone here has experienced the use of this process when a member of the community identified a vulnerability with Adobe Connect. During an ICANN meeting, ICANN's Adobe Connect systems were taken down. So, this is an example of if someone identifies an issue, they can submit their information in, and ICANN security, and other parts of the organization, can work with that researcher, or work with that organization, to then do a managed disclosure of those issues. And we're also seeing greater coordination and collaboration with law enforcement agencies, public safety entities, and others.

After there's an incident, ICANN representatives, often, and community members, present a different event, such as the symposium we had in Thailand. There's also another group that ICANN participates in, called the DNS Operation, Analysis, and Research Center. And this type of information is presented at network operator group meetings, other sessions. And then the ideal is that organizations may use this information to, perhaps, provide some policy updates, updates to contracts, and to maybe redevelop protocols.

So, we're at the end. I want to provide time for questions, so hopefully we're on time. So, key takeaway is to keep mind that the DNS isn't just this technical function—that also it's a key part of infrastructure for organizations. And pay attention to your DNS infrastructure. All of your systems and networks, information, and data could be at risk. The last slide is just some ICANN recommendations that were published in February of this year. And now, we're at the question time. Hi.

JOANNA KULESZA: Perfect.

PATRICK JONES: Are you managing the queue, or do you want me to?

JOANNA KULESZA: I'm happy if you do it, thank you. Thank you very much, Patrick. That was most useful. You've done a wonderful job of combining the technical and the societal challenges we have in cybersecurity. I'm going to use that presentation, in terms of capacity building, to make a call out for pen holders or supportive pen holders for the root server system comment that is still open. We talked a lot about policy development yesterday. That is your chance to get into the work, so to speak, if you're as passionate about cybersecurity as those here at that table.

I wanted to compliment the GSE team. They are wonderful in providing that kind of information. Patrick is great. I've been working closely with the European Outreach Team. If you need that kind of information in your region, I am certain they will provide as much assistance as is possible. I wanted to acknowledge León joining us. I'm really happy you're here. I know the board is doing a lot also, when it comes to cybersecurity. If you have any comment, I would be thrilled to give you the floor—if you have any comment on behalf of linking this work here with the work that the board is doing. And then, I have a queue. I see the queue, and then we'll move to the questions. León?

LEÓN FELIPE SANCHEZ AMBIA: Thank you very much, Joanna. I'm going to be pretty quick, so as to give pace to the questions that might be on the floor. Yes, you are right. This is one of the top priorities for the board. ICANN's mission is, of course, to guarantee the stable, secure functioning of the internet. And this has been embedded to our five-year strategic plan. This is one of our five strategic objectives, and we have designed a series of strategic objectives and goals that will be included in the operational plan that will be designed by staff, in order to implement this strategic plan. So, yes, we hold this security principle, and guaranteeing the secure and stable functioning of the internet, as one of the top priorities for the board in carrying out ICANN's mission.

JOANNA KULESZA: Thank you so much, León. So, I understand that us understanding this better, and supporting you in your work, would also be useful—would also be helpful.

LEÓN FELIPE SANCHEZ AMBIA: Absolutely.

JOANNA KULESZA: Thank you so much. So, I have a short queue that includes Hadia and Holly, in that order, I think. I didn't see the flags going up. I'm wondering if we have any questions from the floor, because the point is to make this as inclusive … Sorry, Judith. Yes, I have Judith. Apologies. Am I missing anyone else? I have Eduardo, brilliant, and I have Holly and Hadia. And I have Javier, brilliant. I'm wondering if there's anyone on the floor, that's not an ALAC member on At-Large leadership, that has questions. Alright, so think about your questions. I'm going to go through the queue, so I have Hadia, Holly, Judith, Eduardo, and Javier. I would ask for a two-minute timer, since we are short on time—a two-minute timer, if possible. Brilliant. Alright, so let's start with Hadia, and then we'll move on. Thank you.

HADIA ELMINIAWI: Thank you, and first I would like to compliment you on all your effort, and the brilliant work, and workshops, and capacity building that you're making in this regard. My question is, taking into consideration that we have international agreements like the Budapest Convention on Cybercrime, does ICANN have any kind of obligations to work with those combatting cybercrime—not like after an incident happen, or to tackle a precise incident, but to collaborate or work with those combatting cybercrime?

PATRICK JONES: Thank you. So, ICANN's not a government, but we do collaborate when we're asked and requested. We do work closely with different institutions and governments, when these types of attacks come to our knowledge. It's in our bylaws, as I mentioned, but our contracted parties are also subject to different jurisdictions. So, when events occur, and we're requested we do collaborate. I don't know if … we're not a signatory to any legislation such as that, but hopefully that helps.

HADIA ELMINIAWI: My question was also related, collaborating in terms of data, of course, and information.

JOANNA KULESZA: So, Hadia, let's note that. We'll note the data context to that. I know that there is more questions coming, so let's just leave it at that level. Holly, a question?

HOLLY RAICHE: It's really a follow-on, and it's probably two questions. Specifically, because there's a lot of debate as to who should actually have access to the data, how do you define a person who has access to the data? What I'm hearing from you is it's not just law enforcement agencies. I'd be interested to know, and maybe talk to you offline about who that is.

My real question … Actually, that's a real question, too. The presentation on DoH and DoT yesterday … We had a presentation last ICANN meeting, the two threats. The first is, you have the packets tunneling below the security systems, or whatever, that have been put in place by corporations. So, in fact, there seems to be a loss of security because the packets are evading or tunneling under the protections that have been put in place.

The other threat that was raised… And this was by the presenter—again, I think it was in Kobe—who said, the problem is, by using DoH or DoT, there will be a few favored resolvers. Right now, there are so many resolvers that you can't possibly

attack all of them. If you start to contract the number of resolvers to a few favored ones, you're in fact creating a target. So, comment?

PATRICK JONES: So, if it hasn't been said already, you'll be hearing from SSAC that they have a work party that's looking at DoH and DoT, and other related issues. They're at the early stages, but this will be an attempt to provide some level setting for the community about what these technologies are. And then, it's up to the different community groups to take up their next step. So, at least, from a community perspective, there'll be some factual information that can help provide a guidance to the different groups about this.

JOANNA KULESZA: Thank you. Thank you very much. I have Judith, Eduardo, Javier. I hope that order is okay. So, I'm going to start with the lady. Judith, go first—two minutes.

JUDITH HELLERSTEIN: Thanks so much for very insightful presentation. I actually have two questions. One is, what is … in an effort, we want to get DNSSEC implemented by many different groups. Is ICANN, maybe, in collaboration with other I-stars, going be working and creating an awareness campaign to get DNSSEC implemented—

and maybe on the line of like what we had, Let's Encrypt, Let's DNNSEC—and trying to get less expensive versions, but still very secure versions, of DNSSEC, so that we can erase that hurdle of organizations not going with—the smaller groups and non-profits not going with DNS, from that issue.

And then, the other one is, an awareness campaign of how to protect the system, and maybe working with the CIOs and others to implement the policy of not sending links in their email. I know you and I have, but …

PATRICK JONES: Sure. So, as León mentioned, and I mentioned in the presentation, security is a key part of the new strategic plan. And there will be work related to DNSSEC awareness and encouragement. I'd say, just watch the space. This will be an area of active work.

JUDITH HELLERSTEIN: León, did you have any … Also, maybe León knows an other thing about trying to something like Let's DNS, like the program, Let's Encrypt, that was a work of a lot of different I-Stars and other groups, and trying to get DNS more implemented by having an inexpensive version of these certificates.

LEÓN FELIPE SANCHEZ AMBIA: Do you mean DNSSEC deployment?

JUDITH HELLERSTEIN: Yes.

LEÓN FELIPE SANCHEZ AMBIA: Well, that's part of the strategic plan, in terms of security. I am not the best technically-qualified board member to speak about that, but I am pretty sure that my colleagues on the Board Technical Committee have been talking about this, and they will liaison, of course—coordinate with staff to try to find the best way possible to have wider deployment of DNSSEC in the most cost-effective way.

PATRICK JONES: Just a quick response, also. There is a effort that's not connected to ICANN called CRYPTTECH, and it's an effort to build a much cheaper hardware security module that then organizations can take and implement DNSSEC. So, right now, if you go purchase one of these, they can be very expensive. And this is an effort to make the process more cost-effective for implementation.

JOANNA KULESZA: Thank you. Eduardo?

EDUARDO DIAZ: Thank you. This is question out of curiosity. Has ICANN been hacked in the past, other than the Adobe thing?

PATRICK JONES: Well, I'm not going to speak on behalf of our DNS Engineering team, but there have been announcements of different issues that have occurred in the past. We'll point you at that part of the organization.

JOANNA KULESZA: Thank you. Thank you, Patrick. Just to note, to Eduardo's question and Judith's, those are all themes we can take up on and discuss further with ourselves, so think you for flagging those, as well that data issue. Javier?

JAVIER RÚA-JOVET: Thank you, chair. Patrick, a great set of slides. Thank you. Question, can you walk us through a little bit, how a sovereign government or an IGO asks ICANN for help—how they engage ICANN. Is it a letter to Göran? How does that work, step-by-step, just a typical case, when they ask for help on something within our agreement?

PATRICK JONES: Sure. So, I mentioned that ICANN is a member of the Forum for Incident Response and Security Teams. Other governments have computer security teams that are also members of FIRST, and that is one channel where queries come in to us. The staff that are part of our Office of the CTO team are also connected to trusted community groups, where information is shared between different government organizations, law enforcement agencies, and others. And so, that's the channel that tends to come in. Perhaps Göran may receive a letter, but those would be published on our correspondence page. The communication tends to occur at the CTO team level.

JOANNA KULESZA: Thank you, Patrick. I'm wondering if there any questions, especially from the open audience. Okay, I have a general question I would like you to possibly use to summarize our meeting. We still have a few minutes. If any questions come up, just let me know. You mentioned that the DNS stops being just a technical issue. That is my understanding, as well, that the question of security transfers from the very technical perspective we've had here at ICANN for a very long time, onto content issues or societal issues. We have got members in the room who are most interested in content, right?

So, that cybersecurity debate we've been having seems to go beyond the strictly technical picket fence that ICANN wants to maintain. So, my specific question is where do we draw the line? Where does ICANN stop and content security begins? Or, to be more general, how do we approach that challenge?

PATRICK JONES: So, that's where I think understanding the contractual relationships is key, because some issues are not directly related to ICANN's role and work but have a direct impact on a particular registry or registrar. So, we have to identify where in the sphere the issue sits. Does it sit as something that's discussed within the GNSO, or is it a wider issue that this group and the GAC can be concerned about? I think that's where those … the conversations have to happen in the appropriate place.

And a key thing to understand is these types of attacks are occurring. It's becoming more prominent. Everyone relies on their phones to connect out to other systems. And so, it becomes an issue where you have to do proper updates on your machines, of your software. Make sure you protect your passwords. Make sure you are keeping up with the latest trends. And start by protecting yourself, and then identify where those issues need to be discussed.

JOANNA KULESZA: Those are very practical guidelines for our users. I'm not going to dive into the data debate. I think it's a topic for a different discussion, so I'm just going to stop it here, unless Hadia wants to, because we still have a few minutes, and I'm interested as well.

HADIA ELMINIAWI: No, I have nothing to add. Thank you.

JOANNA KULESZA: Alright, brilliant. So, I'm going to stop here. If you have any … Oh yeah, even. Sorry, go ahead.

EVIN ERDOĞDU: Thank you. Speaking on behalf Remmy Nweke. He has a question. "Hi. I would like to know if ICANN has specific support plan for ALS promoting DNS for women in Africa."

PATRICK JONES: So, our Africa Engagement Team has worked with the community to have a regional engagement strategy, and I believe security is one of their pillars. So, sharing of information fits within that, and I would point you to the team that's on the ground. So, here, we have Pierre Dandjinou, Yaovi Atohoun, and Bob. Bob is based in our Nairobi office, so that would be the place to start for information that is for the local community.

JOANNA KULESZA: And I already said—I'm going to advertise it again—my personal experience is that the GSE team is always most welcoming. So, if you guys have a location, or if you have a venue, where that information could be shared with your local community, for you to take that feedback back to us and facilitate the discussions we're having to equip León with good guidelines, that's most welcome. I see a question from the audience, if you could … I'm not sure we have a roaming mic, so I'm going to ask you to approach the table, and just use any mic that is on the table. Thank you so much, sir.

CRAIG JONES: Yeah, hello. Craig Jones from INTERPOL. I'm a new Director of Cybercrime. I'm very interested in the prevent approach. We are very quick to try and detect, and we all now that's quite costly—quite resource-intensive. So, from our side—from the global side—we're looking at the prevent side, and how we can do that. So, I'd be very interested to have a conversation as well. Thank you.

PATRICK JONES: Thank you. I'm sure you've talked with John Crain or Carlos Alvarez, and others within that team. Champika, from our APAC

team, presented recently at the INTERPOL event in Korea. So, you know who to talk to.

JOANNA KULESZA: Alright, so I understand that there is knowledge behind, but we're more than welcome to learn that. I see questions. There's a question right there. Is there any other question that I'm missing? No? You might want to use the mic that's right there. Thank you, sir.

MATOGORO JABERA: Yeah, thank you. I really appreciate for the good presentation, and I just want to mention that I'm also representing ALAC to the current ICANN Security, Stability, and Resilience team—that we are conducting a review on the security and stability, resilience of [inaudible]. So, I did appreciate for the point that you have mentioned. And this will also have some input to what we are currently doing. Thank you.

JOANNA KULESZA: Thank you very much. Do we have any other questions? If we do not, I'm going to close the session. I'm going to start by thanking Patrick for the insightful information, and to … I'm going to thank León for taking the time in his busy agenda to join us. I want to thank everyone that joined us for this session. If you do have

questions, and you're just shy, and you don't know how to get involved, just let us know. [Either] email, contact the staff, or contact myself, or just come up to me and talk.

I'm going to advertise the call for pen holders on the root server security comment. That is your first, but not last, opportunity to get involved into ICANN policy—At-Large policy making. Thank you for participating. Thank you to the technical staff and thank you to our wonderful interpreters that we always make such wonderful use of. Thank you so much everyone. Have a good afternoon.

[END OF TRANSCRIPTION]