CLAUDIA RUIZ: Good morning, good afternoon and good evening to all. Welcome to the fifth and final webinar of the five mandatory ATLAS 3 webinars. Today's will cover cybersecurity basics. Our presenter today is David Huberman, Senior Technical Engagement Specialist. We will not be doing a role call for this webinar, however we are taking attendance for the first 10 minutes of this call, after that, your participation will not be a valid entry for the required attendance matrix. If you are only on the phone bridge, please join the Zoom room as soon as possible, as this is an attendance requirement.

We have French and Spanish interpretation for this webinar, so a kind reminder to please state your name when speaking, to allow the interpreters to identify you on the other language channels as well as for transcription purposes. Please also speak at a reasonable speed to allow for accurate interpretation. All lines will be mute during the presentation and opened for questions and answers at the end of the presentation.

As you have noticed, we are running this webinar on Zoom, the features are similar to Adobe Connect but in order to view the participant list and chat pod, please click on the bottom of the screen. You will only be able to see the chat transcript from when you joined the call, nothing prior to that. To raise your hand, please just click on the raise hand icon. I will now hand the floor over to Joanna, co-chair of the ATLAS 3 capacity sub group. Over to you, Joanna.

JOANNA KULESZA: Thank you very much Claudia. Thank you everyone for joining us for the first addition of the last ATLAS 3 webinar, where attendance is a requirement for your participation within the ATLAS selected group of participants. Without further ado, I would be happy to hand the floor over to David, the Senior Technical Engagement Specialist within ICANN.

Thank you so much for joining us, David, we are all excited to listen to your presentation. My understanding is that the participants are encouraged to ask their questions during the presentation in the chat box and then I will leave it to you David whether you want to pick them up after the presentation or during it as you go to decide. Over to you, David. Thank you.

DAVID HUBERMAN: Hello everyone. I'm going to give a fairly brief presentation to you today and then we will have plenty of time for questions afterwards. During this presentation however, I'm not going to keep chat open, as I would like to concentrate on giving a good presentation.

Welcome, we are talking today about cybersecurity and the ICANN ecosystem. My name is David Huberman, I am a Senior Technical Engagement Specialist in ICANN's office of the CTO. I've been on the front lines of cybersecurity for approximately 21 years.

This webinar will be a supplement to the official courses that already exist on ICANN Learn. This webinar, this presentation, is our delivery of the challenges for the ICANN ecosystem with cybersecurity and others in the ICANN Org might deliver these materials in slightly different ways and that's okay.

To begin, I wanted us to think about what things we might commonly find inside a network, a company's network, a universities network, perhaps a government network. Some of the interesting things will find include mail servers. Male servers are not just for email. Modern mail servers have emails certainly, they also have calendaring, all the meetings that we schedule and the appointments that we have. The often include our contacts. Information about us and information about the people in our network.

Another common element we find inside a network are things like database servers. Database servers have a wealth of information. Data about assets. Data about customers and sometimes even data about employees.

Another common element, there are file servers and on file servers is all the information about financial information, spreadsheets, design documents. It's where we can find information about our organizations processes and procedures.

This seems very straightforward, there's really interesting information you can find inside any of these networks. Underpinning these elements is actually some really interesting stuff. We have things like identity management. To access our email. To access the file servers and the databases, we have to go through processes that authorize us to do so, who can see the data? Processes that authentic us, what is our username, what is our password and for multi factor authentication, what is the security token that we present in addition to our password? When you're managing these systems you also have to manage the keys. The username and passwords certainly but also the key fobs, the

cryptographic keys and all the secondary tokens that help us to keep our systems secure. We also have to engineer these systems, they live on hardware, they're run by software and both hardware and software require up to date patching.

More deeply inside these systems is the is the routing infrastructure. It's our connectivity within our network and it's our connectivity to other networks outside of our company, outside of our university, outside of our government. With this connectivity and in this infrastructure are the key elements of IP addresses and the domain name system, the DNS.

Finally, when we're running all these systems there's a governance component. There's a security policy, who can asses this data and how do they access this data? Then there's policy on data storage, what do we store, where do we store? And data retention, for how long do we store it?

The reason I'm talking about all this is because it is these elements that are under attack constantly by people who are trying to find the vulnerabilities in each of these things that you see on your screen. The vulnerabilities because if they can compromise these, they can get to those key systems and steal the data. Common ways they do this include things like phishing. I've put in a dictionary definition of phishing, which I found to be very good. Phishing is the fraudulent practice, sending emails that report to be from a reputable source, in order to induce and individual, to reveal personal information, such as a password or credit card number.

Another type of attack is malware and this is software that is specifically designed to disrupted, to damage or to gain unauthorized access to a computer system. Some common modern types of malware include ram simware and keystroke loggers, root kiss and viruses.

Then we get more complex with things like botnets. Botnets are a network of private computers infected with malicious software, infected with malware and controlled as a group. A botnet can be thousands or hundreds of thousands or millions of computers all around the world, that are under common control, that are used to conduct attacks.

A very important type of cybercrime that we talk a lot about, that we'll talk about here and we'll talk a lot about in the ICANN ecosystem is what we call DNS Abuse. The DNS is everywhere. DNS is used all the time to resolver user friendly names, to internet protocol, IP address. It turns out, if you disrupt the DNS, you can disrupt a lot. You can disrupt merchant transactions. You can disrupt government services. You can disrupt social networks and many, many other things. If you exploit the DNS, you can trick, defraud and deceive users. Common ways you can exploit the DNS are to maliciously register domain names. To hijack the name resolutions or the registration services that service those domain names. Of course, you can corrupt DNS data at its source.

I don't want to talk about this just in the abstract. I want to talk about this, what this looks like in the real world. Today we can share two explains of some very, very recent cyberattacks that have happened. The two types of attacks I'm going to talk about include targeting vulnerabilities in the internet's routing system and in email systems that were run by targeted companies. Any cyberattacks involved a lot of

DNS Abuse and primarily, these attacks surreptitiously, behind the scenes, they altered name resolution in ways that targets, the victims didn't even know about.

The first attack was on a service, was on a crypto currency service called MyEtherWallet.Com. MyEtherWallet.Com is a place where people who own thorium can store the crypto currency. Attackers were able to use routing hijacks to redirect some DNS queries. By doing these things, they were able to trick and deceive users into inputting their login credentials for the real MyEtherWallet.com website. Once the attackers were able to deceive the users, they were able to then steal approximately 21 million dollars of crypto currency from the real My.Ether.Wallet.com.

The second, very recent set of attacks has two names, DNSpionage, which happened at the end of 2018 and an attack that is currently still ongoing, that's been dubbed by the security community with the words Sea Turtle. These attacks are not for money. Unlike a lot of cybercrime, which is motivated by making money, these are actually political attacks. These are what are called Military Cyber Offence Pre-Positioning. Gathering all the intelligence needed to launch future military cyber-attacks. DNSpionage and Sea Turtle have affected 40 organizations in 13 countries in North Africa and the Middle East. Targeting primarily national security organizations, ministries of foreign affairs and some large and significant energy companies. They do this by infiltrating the DNS and email and things like certificate authorities, which are used as validation tokens commonly on websites.

These types of large-scale attacks that I've just described, they're infrequent but because of their surface area, because of how big and how much they infiltrate, they wind up involving things like sovereign governments, multinational companies, international law enforcement of course gets involved and we get to read about things through wide spread news coverage. Outside of these infrequent large attacks, every single day there are other, smaller cybersecurity incidents happening all around the world.

Today, we're going to note that the ICANN Community and that's you and members of the ICANN Org, Staff members, have a role in these cybersecurity incidents. We have roles before, during and after them. During this webinar we'll describe the ICANN Community and the ICANN Org's role in the cybersecurity ecosystem and while doing so, we're going to help familiarize you with some key cybersecurity technologies.

Let's begin with all the things happened before any cybersecurity incident occurs. It is ICANN's Bylaws, it is ICANN's Mission, that places a strong emphasis on cybersecurity. Quote, the mission of ICANN, is to ensure the stable and secure operation of the internet's unique identifier systems. Inside of our bi-laws there are many commitments that the ICANN Org has made. One of those is to preserve and enhance, the administration of the DNS and the operational stability, reliability, security, inter-operability, resilience and openness of the DNS and the internet.

We have these terms that I highlighted in the slide, security, stability ad resiliency. These are terms that you are going to hear a lot, all throughout your time in the ICANN ecosystem. At meetings, on mailing

lists, in working groups, in discussions. It's about the security, the stability and resiliency of the internet and of the unique identifier systems that ICANN helps coordinate. We often abbreviate these three terms with the term SSR, the internet's security, stability and resiliency.

What do these terms mean? They're pretty straight forward. Security is the capacity to protect and prevent misuse of unique identifiers. While stability is the capacity to ensure the system operates as expected and users have confidence that they system operates as they expect it to. Resiliency is the capacity, the capacity of the unique identifier system, to affectively withstand malicious attacks and other disruptive events without cessation of service.

In fulfilling our commitments to the SSR of the unique identifier system, I feel like we focus our efforts in three different arenas. A very big and important arena is policy development. One is identifier operations and everyday and every week, we are participating in capacity building efforts, to inform and make people aware of technologies and trends in cybersecurity.

Throughout the ICANN ecosystem there are so many communities that work hard to develop bottoms up, multistakeholder policies and procedures, to improve the security, stability and resiliency of the internet's unique identifier system. There are way too many communities to list working on this but I highlighted three of the big ones. The GAC, the Government Advisory Committee, has a public safety working group, the PSWG. The PSWG focuses on aspects of ICANN's policies and procedures that implicate the safety of the public. That safety of the public includes developing the DNS abuse and

cybercrime mitigation capabilities of ICANN and law enforcement communities.

In addition to the GAC's PSWG, there is another large and prestigious advisory committee called the SSAC, the Security and Stability Advisory Committee. This is a group of esteemed internet engineers and security experts, who have been selected to sit on a committee and do threat assessments and risk analysis of our unique identifier system and help ICANN assess where the principle threats to SSR lie.

The third community I wanted to highlight is a very small one, it's the Root Server Operators. The Root Sever Operators gather together under an advisory committee at ICANN called RSSAC, the Root Server System Advisory Committee. The Root Server Operators and RSSAC advise the ICANN Board and the community on matters relating to the operation, the administration, security and the integrity of the root server system, which sits at the top of the DNS tree.

A different part of policy development, that's just as important are the contracts. The contracts between ICANN and the registries and registrars, these are very important tools. I'm going to skip ahead for just a slide but I'm going to come back. We have lots of contracts in the ICANN ecosystem. Looking from left to right at the bottom, you can see that between ICANN and the registry of a top-level domain, we have a contract called the Registry Agreement.

Between the registry of a top-level domain and the registrars, who actually register domain names for individuals, is a registry registrar agreement. At the top, between ICANN and the registrar is this

accreditation agreement, how to qualify and what responsibilities you have to be a registrar. From the registrar there are agreements with the reseller, resellers and the registrant or perhaps just the registrant and the registrar directly have the registrant agreement.

Moving back to the previous slide, I wanted to highlight two of the big contracts and how they're relevant to this discussion today. The agreement between ICANN and the registrars, that give accreditation to a registrar, it actually imposes a contractual duty to investigate abuse when abuse is brought to the registrar's attention. The registry agreement between ICANN and a TLD registry includes a provision that in the registry/registrar requires registrars to include in the registration agreement a provision that prohibits registered name holders, registrants from distributing malware, abusively operation botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging activity contrary to applicable law. This is very strong contractual requirements to investigate and prohibit cybercrime.

The second arena in which ICANN fulfills its commitments, is identifier operations. ICANN has a subsidiary, an affiliate company called Public Technical Identifiers and you'll always hear that references as PTI. PTI is responsible for the operational aspects of coordinating the internet system of unique identifiers. It does so by carrying what's called the IANA Function.

The IANA Function has three very important prongs. The first is about resources. It's about allocated IPB4 addresses, IPB6 addresses and something called Autonomous System Number AS Numbers to the

RIR's, the Regional Internet Registries that register and hand out addresses and AS numbers to the companies around the world.

The second important prong the PTI manages are DNS operations. They do a lot in this and I've highlighted three. One is to maintain the root zone for forward DNS. Another is to administer the. RPA for reverse DNS. Then this very technical term, is to maintain the trust anchor for DNSSEC. I've highlighted DNSSEC because we're going to talk about that, so we have some basic understanding of what it is and why it's important today.

The third task that PTI has is something called Protocol Parameter Registry, the Internet Engineering Taskforce is a community group that works on and creates and publishing the protocols, the base protocols of who the internet actually operates. Those protocols have parameters. A protocol might say that the number one means this, the number two means that and the number three means this other thing. It's very important that you define the parameters and you publish them somewhere so everybody can see them. PTI publishes these parameter registries and they actually have over three thousand of them that you find on the PTI website, of all the different protocol parameters.

I want to talk very briefly about DNSSEC. DNSSEC stands for the Domain Name System Security Extensions. The purpose of DNSSEC is to help prevent DNS abuse. It does this by introducing cryptography. This cryptography provides assurances to users of the DNS, that the data they are seeing is valid and is true. Domain Name Registrants, someone who owns a domain name and runs it, signs their DNS data and says,

"This is my domain name and this is the DNS data about this domain name that I have published."

DNS Operators valid that information as the DNS data passes through their resolvers. DNSSEC uses keys; it's called Public Key Infrastructure PKI. We have a lot of terms here but very briefly the Key Signing Key, the KSK is the top most key in the hierarchy of DNSSEC. It has a public/private keypad for the public part, is the trusted starting point, trusted by the entire internet for DNSSEC validation. The private part signs the next key in the hierarchy called the Zone Signing Key. The purpose of this is all to build a chain of trust. It's a chain of trust of successive keys in a hierarchy, with signatures that can be used by everyone to validate the authenticity of any DNSSEC signed data. By signing this data and by validating this data, we help end so much of the possible DNS abuse.

With all that comes PTI's role in DNSSEC. PTI is entrusted by the entire internet to issue, manage, change and distribute all of these keys. Not only that, they're the ones who sign, cryptographically sign these key sets. PTI does all of this by ensuring that it follows cryptographic best practices that have been developed by the Internet Engineering Taskforce, the IETF.

The third prong in fulfilling our commitments is about capacity building. Community members of ICANN, staff members of ICANN, almost every day we regularly participate in efforts to teach organizations all over the globe, on matters relating to the unique identifier system that ICANN helps coordinate in cybersecurity. We do this to increase knowledge

and awareness. We do it many different ways, in many different forms, that' includes webinars, like we're having today.

When you got to an ICANN meeting, you'll find sessions that are on the schedule called How It Works. Many different sessions that will go into detail about different technologies so that you can have a good understanding of what they are and how they work. We conduct technical workshops over many days or even full week technical workshops. We give many trainings to global law enforcement agencies across the world, to help them understand these technologies, understand the methodologies that attackers use and understand how to help stop cyber instances and many other types.

That's what happens every day in the ICANN ecosystem and we think of these in the context of before anything happens. What is ICANN's role, what is our community's role during a cybersecurity incident? When a cyberattack is going on, what we want to do is we want to stop it. Stopping it requires a large coordinated response from many different actors. Those actors include the network operators, these are the service providers for the enterprise networks which the cyberattacks are using or abusing to conduct its operations.

Of course, stopping the cyberattack requires help and a response from global law enforcement agencies. It needs the help of these things called CIRTS, Computer Incident Response Teams and CIRTS are very commonly organized at the National level, I list them here as National CIRTS. The other thing we need help with when we're trying to stop a cyberattack are the registries, the domain name registries but also the IP address registries, the IRI's. We need the registries help because

attribution. In order to stop an attack, you need to know who is conducting the attack. What networks and what resources they're using in this attack. We need know who is the registrants of the IP addresses being used in this attack.

We also need to know who's the registrant of the domain names that are being used in this attack. In order to answer these questions, we need registration data. The registration data are the data sources from which we are able to conduct attribution. These data sources are the registration records for IP addresses and AS numbers and these are found in the IRI's, the Regional Internet Registries and we need the registration data for domain names.

ICANN Org itself has a coordination role. ICANN has a team inside the office of the CTO. When you're in ICANN Meetings and on ICANN mailing lists, you'll see the office of the CTO referred to by our nickname, OCTO and this team works with all these organizations during a cyberattack to coordinate the responses. They do this because these are professionals with very deep understanding of cyber crime from both perspectives, attacker's perspectives and responders' perspectives.

ICANN's team has very strong connections to global law enforcement and importantly, to the operational security community, OPSEC, the Operational Security Community of the Internet Network Operators, who are on the front lines of cyber instances. ICANN's team uses this very deep understanding and strong community connections, to bring all of the parties together when we're taking down cyberattacks.

Separately, our coordination role includes this process we've developed called the Coordinated Disclosure Process. This is a process that anyone, a security researcher, registries, registrars and anyone in the community can use to report vulnerabilities and bugs that they have found and report them to ICANN, so that ICANN can work with all of the relevant parties to fix and patch the venerability's and bugs to prevent future crime.

When it's all over, it's time to take a look at what happened. There's a lot that goes on and to figuring out what happened, what went wrong? People take a look at the vulnerabilities that were discovered, the bugs that were found. They may write up some research, they may write some papers and what really happens is we talk about these things in conferences. We talk about these things in face to face conferences and sometimes in virtual conferences, where we all want to understand what happened and identify the vulnerabilities that we need to fix. There are many different conferences where these are discussed. I wanted to point out three really interesting ones.

One of them is the annual ICANN DNS Impose, where the four most DNS experts in the world gather together every year to talk about what the relevance of the DNS with cybersecurity at the time.

Another is another DNS conference called DNS OARC and really importantly is this concept called NOGS, Network Operator Groups. These are national, local, regional groups that have communities that have come together or network operators, who want to share information, share awareness and help each other to operate their networks better.

Once we've talked about what's happened, once we've identified bugs and vulnerabilities, then it's time to adjust the ecosystem to harden to make more resilience, the internet, against these types of attacks. Maybe different things might be necessary. It might be policy updates. We might need to go to PSWG or SSAC or RSAC or many of the other communities and say, "Hey, we found some holes and policy can help plug those holes, so let's work together to do that." We may need to update contracts that exist in the contract ecosystem, to better handle and make everyone more responsible for stopping cyberattacks.

Maybe, we need to go fix -- write new protocols or fix existing protocols. We'll go over to the IATF and share our findings and work together to fix the basic protocols that were exposed during a cyber incident. Then, always with these things, the most important this is capacity building. Going to the community, going to network operators, going to global law enforcement, going to civil society, discussing what happened, discussing what the effects were and everyone having a good understanding of what's going on and what we need to do.

We have some takeaways from what we've just discussed. The first takeaway is that the DNS really matters. I know that maybe sounds a little funny because DNS is such an important technology but it's important to think about, that the DNS is not just a technical function anymore. It's not just this thing that's some system administrator, some engineers who are behind the scenes, who's names you may not even know, they just configure and run in the network and we don't have to pay attention to them.

It's bigger than that now. The DNS is now a critical infrastructure. It's used everywhere, email, web browsing, mobile applications, banking, everything. The DNS is now the gateway to all of the internal systems. The systems we talked about at the beginning of the webinar, the email, the database servers, the file servers, you can try and protect those all you want and you should but if you leave your DNS open, if your DNS is compromised, all of our systems and all of you networks are risk. It's critical, the policy makers and organizational decision makers, pay better attention to their DNS infrastructure.

ICANN has some new recommendations about that. ICANN is strongly recommending; we published a set of cybersecurity measures to harden the local DNS infrastructure against attacks. We have many different steps, I'm not going to detail hem here but the steps are about authorization and authentication, making them stronger and better. Using encryption, patching, keeping your hardware and software up to date and well patched is a very critical to hardening your infrastructure. There're some important steps with email security that everyone needs to take. But beyond all that, there's no surprise when I say that, one of the most important recommendations ICANN makes, it's really, really critical that you implement DNSSEC. The signing and validation procedures inside DNSSEC stops so much of the abuse of the DNS infrastructure and protects your systems.

Our final takeaway is the general concept of the Internet Security and Stability and Resiliency, it's SSR and ICANN. Because cybersecurity is one area of focus of ICANN's Community and ICANN Staff. ICANN defines cybercrime, we include things like malware distribution, phishing attempting, operating botnets, piracy and fraudulent or

deceptive business practices. The time and effort that we put in here at ICANN as community member and as staff members, all this time contributes and the work we do is intended to increase the stability, security and resiliency of the internet and its system of unique identifiers.

I've talked for a bit. I'm going to open up my chat and I really invite you to ask all the questions you have.

JOANNA KULESZA: I can see the chatroom, we have three questions right at the end of the chat box, so if you can see it, you're more than welcome to use them. If you need to me to recap, I'm also happy to do that as well. He's captivated the audience, they held out with the questions till the very end.

DAVID HUBERMAN: Let's see, I'm going to work from the bottom up. Does DNSSEC render AXFR blocking census? DNSSEC is fast but far more resource hungry, so I would recommend to open AXFR in the case of DNSSEC deployment. That's a decision that registries have to make for themselves. There are reasons to allow AXFR, there are reasons you may not wish to allow AXFR. But outside of those reasons is the need to implement -- is our strong recommendation of implementing DNSSEC, allowing the registrants inside a TLD to sign their domains, to sign their DNS data, to that everybody else outside of that registry can valid it. It's really two different issues and the AXFR thing is up to the individual operators.

The second question I see, despite the security in place, why is there increasing cybersecurity threats? A very good question. That's because people have different motivations. A lot of the cybersecurity threats we see are very simple, it's about money. If someone can make money off of you by scamming you, unfortunately there are people there who do that. Very compute savvy people, very, very engineering smart people, have found creative and intrusive ways of using our cyber infrastructure to do cyberattacks.

They like those because they can hide behind a computer, we can't see their faces, we often don't know their names. That kind of anonymity powers people to sometimes do things they wouldn't otherwise do face to face and one of those is steal, to steal money. One of the attacks I talked about, DNSpionage and Sea Turtle, these are things that government actors are using against other government actors for political purposes. In some respects, that's even stronger than monetary incentive because of how passionate people and countries get about politics.

A question just popped up from Vanda, how deep should DNSSEC be implemented? DNSSEC is implemented in two areas, well three areas. It's first enabling, it's enabled by a registry, again registry is responsible for a top-level domain. When the top-level domain is signed by the registry operator, that allows everybody who has a domain name in that registry, in that TLD, to then do their own signing and validation. DNSSEC is implemented by the registry operator, then once that's done, every registrant of a domain name should sign their DNS data.

The other part where it's implemented is by everybody else who has nothing to do with that TLD, nothing to do with those domain names. Everyone who operates a resolver, a recursive resolver, that gets DNS data from everybody else in the world and they simply need to turn on DNSSEC to validate anytime a signed, anytime a DNS signed response comes through their resolver then they're going to pass it off to the end users who asked the DNS questions, they can validate it and they can see this answer is true and it is what it was intended by the domain name registrant.

Eli has asked, what is the responsibility of the registrants in terms of when a user got attacked, compromised or the service provider punishes the users for something that was not under their control? The responsibility of registrants -- I don't know that the domain name registrant, which is a person who owns the domain name, example.com, I don't know how much responsibility they have in this discussion if a user is attacked or if that domain name is compromised.

The compromise often happens at a higher level than the just the registrant. Sometimes it happens at the registrar level, some of the systems the registrar are using. Sometimes it happens higher than that, sometimes it happens at the registry level. There are all sorts of systems that exist between registries and registrars, between registries and ICANN that are vulnerable to attacks sometimes. But all of these are above, they're upstream of the registrant. The registrant doesn't bare a tremendous amount of responsibility in this discussion that we're having.

The next question from Lutz is, does DNSSEC can be responsible for distributed reflection and amplification attacks. Are there any new ideas besides BCP38, a test due with the filtering, inbound and outbound traffic? Reflection attacks and amplification attacks happen because of vulnerabilities inside of systems that have not been properly hardened against them. DSN SEC is about validating that data, DNS data is accurate. I don't really think the DNSSEC is so much responsible for this but stopping -- but even if you disagree, stopping reflection and amplification attacks is about different types of practices that you have in your networks.

Are there any new ideas beside BCP38? That's a very good question. I have to think about that. Good hygiene is important, beyond just filtering of routes, beyond just filtering the traffic that comes in. It's also about hardening systems inside and making sure there are no vulnerabilities that can be used for reflection and amplification attacks. There's a lot of things that go in it. That's a good question.

Wale asks, are there any security schemes offering better security policies other than DNSSEC? DNSSEC is a tool right. DNSSEC is a tool that allows you to protect the DNS data that you're trying to publish as a domain name registrant and allows you as a user of the DNS to simple say, "Oh, good, the response I'm getting is what was intended." But there are many other security schemes and other security policies that network operators and that DNS operators have to implement, many of them. Filtering and things called control lists and firewalls, some basic and some not so basic schemes that exist. There's a lot of routing tools that are available to operators, to help better harden their security, to help better protect them and their users.

David Mackey writes, as a member of NARALO, I'm interested in the perspective of non-technical end users. Good question David. What should end users be aware of with respect to security? Should end users leave security up to experts or is there something end users can do? That's a very big question, that's a great question. In the context that we're discussing today, end users don't have a lot of control over a lot of this but there are things we can do to help protect us so that we're not victims, that we're not part of the problem.

One of the big problems in the internet today are botnets and botnets are made up of compromised computers, the laptop I'm on, my desktop computer in my house, my mobile device, my phone. If one of these or all of these get compromised, they can be used as part of botnet, which can be used to attack other institutions. For me as an end user, it's just important that I keep my stuff locked down. It's important that I don't install software I'm not supposed to be installing or I don't know what it is. It's really important that I train myself to not fall victim to phishing attacks. Phishing attacks are the number one way in which bad guys get into our computes by sending us files that pretend to be from a friend and so we open them up and boom we're infected with malware or get us to click on links that take us to places that take control of our computers.

Maybe even fake websites that we think we're going to and we input our user credentials, our username and our password. It's about being smart. It's about being a smart cyber citizen and doing your best to protect your devices and be very careful about what you allow your devices to access and what you download onto your devices. That's my first answer to your question David. There are others and some of it is

demanding more from our upstream. If demanding better cybersecurity from our service provider. It's being aware and seeing problems and reporting them to the companies we work for or the universities we're at or the governments that we might be part of. It's about when you see something, you say something.

Lutz asks another good question, is the delegation chain able to withstand the attack surface raised by TSLA Cert validations? It can. If you design it well, if you are a registry operator, if you are a registrar, a reseller and you think about how you build your systems between you and the party right next to you, above and below. If you build it properly and if you communicate with each other and if you continually stay up to date, you can withstand these attacks. But it's not easy and I think that's implicit in your question, it's not easy because cyber criminals are very intelligent, they're very good. It's a constant battle and we have to be very, very vigilant.

Wale asks, do you think messaging encryption techniques and the fight in phishing in malware? Maybe. Encryption is a good thing to use but I typically think of encryption as better protecting our privacy. Better protecting in case someone happens to be able to listen or is able to obtain copies that were messages to each other. When they're encrypted and only you as the sender and me as the recipient, have the keys to decrypt those messages. I think that's more to provide protection, excuse me, privacy protection. Does encryption help against phishing and malware? I'm not sure, off the top of my head I'm not thinking of anything but perhaps I'm just not thinking of it right now. Good question.

Just a couple minutes left in our one-hour webinar. If anyone has any other questions, I'm happy to answer. Joanna asks, would you be willing to share your insights on cyberattack attribution with WHOIS gone dark? Does it impact the ability to technically attribute cyberattacks? Everything I'm going to say is my opinion as a network engineer who works here, I'm not giving an opinion that speaks for ICANN, the ICANN Organization. Attribution is a tough thing. Some WHOIS that were available for a very long time are not available right now. Not all of it, WHOIS hasn't gone completely dark but there is some WHOIS information that's not available that use to be.

I think it's a common sense conclusion that would certainly handicap the ability of the responders to attribute what's going on. However, if you really dive into an attack, you actually aren't going to rely on WHOIS quite as much as you might think because there are basic pieces of data that are not hidden, that have not gone dark in WHOIS, such as the IP address, it's eventually registered to some organization, often an ISP or a large company and that information is always available at WHOIS.

Also, the important thing is on the technical, the autonomous system network and that's an identifier, technical identifier that tells you what network it's actually going through. WHOIS the register of AS number is not hidden; it is always attributable. Very good engineers are able to see some of the basic information for attribution and then outside of WHOIS, go to these network operators and start asking questions, "Hey, this IP address was used at this time, at this date to do something, can you please help us find who this was?"

And if you're a government, if you're a law enforcement, you say, "By the way, here's my court order telling you, you must cooperate." So, WHOIS makes things harder and makes things probably slower, WHOIS information not being quite as available makes it a slower process but it doesn't end the process of attribution, we just have to go in different directions.

I'm going to take one final question, helpfully translated, thank you Claudia. Can ICANN have a documentation center for the purpose of keeping members of different communities informed, technicians, engineers, organizations and end users? Yes, we try and do some of that now, the ICANN.Org website has a lot of information on it. I understand, I'm smiling as I say this, it can be hard to find things sometimes. If you go to ICANN.Org/technology, which I'm typing in the chat now, you'll find lots of resources that I hope provide some of this documentation and certainly get you to other very useful links that have this documentation for helping keep everybody informed.

Of course, we also do this, as members of the community and me and my colleagues, as members of the ICANN Staff, we're always communicating with all of the communities, with NARALO and the end users. With policy makers who are engaged in the working groups and in our supporting organization. In our advisory councils. We're doing it on email and teleconferences and face to face conferences. Engineers, very key ones there, that's actually one of the things I do, me David, I go around to different engineering groups, to network operator groups and we talk about what's going on. We work together to try and help solve the problems.

That's it for me. I'm going to turn it back over to our organizers and say thank you everyone.

JOANNA KULESZA: Thank you, David, so informative. I am certain all of the participants enjoyed it, I know I have. Thank you so much for taking the time to join us. Thank you for the most informative presentation. Just a reminder that the presentation itself and this webinar will be available on the At-Large wiki page. For those of you still feel the hunger for more cybersecurity knowledge, there is another addition of this webinar tomorrow, I think that's tomorrow for most of us, it's Wednesday May 22nd at noon UTC. It's going to be Patrick Jones who will pick up this topic again in roughly 12 hours. Thank you so much, David.

To everyone who participated, thank you for taking the time. Thank you to our wonderful interpreters. Thank you to the wonderful Staff who as always, are the most helpful. Feel free to reach out to us if there are more questions or issues regarding the webinar itself. I will stop here. Thank you again, thank you David, thank you everyone. Enjoy the rest of your day.

[END OF TRANSCRIPTION]