ICANN72 | Virtual Annual General Meeting – NextGen Presentations
Monday, October 25, 2021 – 10:30 to 12:00 PDT

DEBORAH ESCALERA: Hello everybody and welcome to the NextGen@ICANN 72 presentations. My name is Deborah Escalera and I manage the NextGen@ICANN program. I am the remote participation manager for this session.

Please note that this session is being recorded and follows the ICANN expected standards of behavior. During the session, questions or comments will only be read aloud if submitted within the Q&A pod. I will read them aloud during the time set by the chair or moderator of the session.

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

If you wish to speak, please raise your hand in the Zoom room and once the session facilitator calls upon your name, our technical support team will allow you to unmute your microphone.

Before speaking, ensure you have selected the language you will speak from the interpretation menu. Please state your name for the record and the language you will speak if speaking a language other than English. When speaking, be sure to mute all other devices and notifications. Please speak clearly and at a reasonable pace to allow for accurate interpretation.

Note: The following is the output resulting from transcribing an audio file into a word/text document. Although the transcription is largely accurate, in some cases may be incomplete or inaccurate due to inaudible passages and grammatical corrections. It is posted as an aid to the original audio file, but should not be treated as an authoritative record.

All participants in the session may make comments in the chat. Please use a dropdown menu in the chat pod and select "respond to all panelists and attendees." This will allow everyone to view your comment. Please note that private chats are only possible among panelists in the Zoom webinar format. Any message sent by a panelist or standard attendee to another standard attendee will only be seen by the session cohost, host and other panelists.

With that, I would like to welcome you to the session and thank our NextGen participants for all their hard work in preparing their presentations. And I'd also like to thank my mentors, Aris Ignacio and Dessalegn Yehuala who've been working tirelessly for the past eight weeks prepping the students and guiding them through this process and helping them to get ready for ICANN 72. They really have been working hard, and I could not have done this without them.

Also, I'd like to thank my colleague, Siranush Vardanyan who will be running the slides today for me. Very much appreciate your help, Siranush. And with that, because we only have 90 minutes and we have six presentations, we're going to start right away and I'm going to hand the floor over to our first presenter, Sarah Alsamman. Sarah, the floor is yours, and we'll follow that up with questions.

SARAH ALSAMMAN: Hi. Thank you so much, Deborah. Hello. thank you for having me. Today I want to talk about DNS and web content abuse, more specifically disinformation. Next slide, please.

For those who may not already know, the DNS or domain name system is an integral system which underpins the Internet's ability to connect its users and devices. Just as other systems are, however, it is prone to abuse. As stated by ICANN's very own Governmental Advisory Committee, those entrusted with administering the DNS infrastructure must take the steps to ensure that this public resource is both safe and secure.

This is important for the public to be able to trust and rely upon the Internet for crucial communications and transactions. So my goals in this presentation are to encourage dialogue in the stakeholder community on this important public policy issue and to also encourage the ICANN community to continue disrupting abuse in, with and around DNS as a whole.

But before DNS abuse can be properly addressed, registrars and registries need to have a shared understanding as how to define it. Next slide, please. So according to the Internet & Jurisdiction Policy Network's DNS abuse framework, there are five key forms of abuse that have already been identified. These are in the cases of malware, botnets, phishing, pharming and spam.

There is also the case of content abuse, which is not technical and therefore it needs its own distinction. In order to protect freedom of speech, registries and registrars are usually not required to act on web content abuse. However, the GAC framework agrees that there er specific cases where actions should be taken and these are in the cases of child sexual abuse materials, illegal distribution online of opioids, human trafficking, and specific and credible incitements to violence. Next slide, please.

So now that we have defined content abuse on the DNS, I want to introduce the issue of botnets which operate on social media. As I'm sure we can all observe today, data processing algorithms are becoming increasingly influential instruments of our perception, of our realities. Most common are bots working for political actors which are then able to manipulate public opinion over major social networking applications that we use every day.

The botnet’s ability to steer the construction of public problems has a direct impact on the perception and ordering of our own social and political realities. We see this most often with computational propaganda, and studies have shown—as the one that I'm going to present in the next slide—that they're more likely to appear during or after a crisis, distorting it and creating more damage around that specific crisis.

Because moments of crisis generate a collective uncertainty on the masses, this renders audiences on these networks as highly influenceable. Next slide, please.

So the British Journal of Sociology did a study on communications through Twitter and Facebook after the Manchester bombing, which was a terror attack. In one case, a woman’s Facebook account posted that she was housing over 60 lost children. This post also had her phone number attached and quickly circulated throughout Twitter. The content spread enough that she was eventually labeled as the angel of Manchester by the Daily Mail.

But the problem is that this event never actually happened. This is what we would call event ghosting. The woman explained to the police later that she never made the post or even issued her phone number, and claimed she was very shaken by the incident as she was getting numerous calls throughout the night. 28 separate ghost incidents such as these occurred the same night, adding to the chaos in aftermath of the bombing. Next slide, please.

Another separate incident online that night, a Facebook post was made claiming that there was a shooter at Oldham hospital with people locked inside. This post was made moments after the bombing and shared by at least 368 accounts on Twitter after screengrabs were taken from Facebook. The hospital denied this rumor, yet this false information continued to circulate in the very crucial hours that followed the terrorist attack.

Because of this specific ghost event, some emergency crews had to stay behind following false trails such as these. What makes situations like these so dangerous is how the safety of communities can be impacted at such a large scale when social networks can actually disrupt communication between emergency services and then the publics that they serve. Next slide, please.

So clearly, website content abuses can pose a threat to human life and civil safety, therefore they should be discussed for policy in the future. Actions to incentivize the adoption of proactive anti-abuse measures in new or developing registry agreement provisions should be made to ensure the safety of the Internet and the community of its users in the future. Thank you.

DEBORAH ESCALERA: Thank you, Sarah. Very well done. Okay, are there any questions for Sarah? I don't see any. You can always ask questions at the end if you find something comes up. With that, we'll move on to our next presenter, Meri Baghdasaryan. Thank you.

MERI BAGHDASARYAN: Thank you, Deborah and Siranush. Good morning, good afternoon, good evening. My name is Meri Baghdasaryan and I'm a recent master of law graduate from University of Pennsylvania law school. My interest in privacy and policymaking at ICANN brought me to the topic of today's presentation, namely privacy and proxy services accreditation. Next slide, please.

In 2013, the ICANN Board approved the new registrar accreditation agreement, or the RAA, which is a contract that covers the relationship between the ICANN and its accredited registrars. As we would see, the provisions of this agreement have impact on registrants and other third parties involved in the domain name system.

In initiating the negotiations of this agreement between ICANN and the Registrar Stakeholder Group back in October 2011, the ICANN Board has also requested an issue report from the GNSO that upon the conclusion of the negotiations, the GNSO started a policy development process to address any issues not addressed during these negotiations. And issues related to privacy and proxy services were identified as one of those remaining issues.

The 2013 registrar accreditation agreement actually contains a temporary specification that covers registrars' obligations with respect to privacy proxy services. The deadline for this temporary specification has been extended a few times already and currently, it is set to expire on 31st of July of 2022 or when the ICANN implements the new accreditation program, whichever occurs first.

But before we proceed, let's understand what we mean by privacy proxy services. Currently, these are defined under the mentioned specification. So a privacy service allows a domain name registration in the registrant's name but all other contact details displayed in the publicly available registration data directory service are not actually given by the privacy service provider and not by the registrant.

And in case of a proxy service, this service allows the registered name holder to license the use of the domain name to a customer who actually uses the domain, and the contact information in this directory is provided by the proxy service provider. Next slide, please.

Under this specification, that is the one in force right now, we have a minimum set of requirements that are applicable to privacy proxy services. The four main minimum requirements include the disclosure of key service terms, the publication of infringement or abuse point of contact, publication of business contact information, and escrow of customer data. As we see, the specification attempts at addressing the handling of this nonpublic registration data. Next slide, please.

But why are we even discussing this topic? Why is this important? So if we go back to 2011, when the ICANN Board requested the issue report from GNSO, the ICANN Board also highlighted the urgency of addressing this issue with the privacy proxy services, because this would provide greater protection for the registrants and it will reduce DNS abuses.

So since then, this issue has actually become more persistent and has even been exacerbated during the pandemic. For instance, during the ICANN 68 GAC session on DNS abuse, it was noted that 65% of the domains used to defraud people during the pandemic were hidden through privacy proxy services. Moreover, some practicing attorneys also raised the alarm that after GDPR entered into force, the number of WIPO UDRP complaints against DNS abusers increased significantly, and most of these complaints involve persistent lack of compliance to reveal the contact information from privacy proxy service providers. As a result, registrars or their affiliated proxy providers require IP holders to file UDRP actions or obtain a court ordered subpoena in order to receive the contact information of the DNS abuser.

It is clear that this raises a lot of unnecessary concerns with regards to taking more time to go through the simple procedure as well as spending more resources to obtain the contact information to move forward with their complaints. In other words, the accreditation will actually help to advance the registrant protection to reduce DNS abuse as well as to decrease the number of UDRP complaints. Now let's go back to ICANN Board's request to issue a report from GNSO and discuss what happened after [that.] Next slide, please.

So on this slide, we see the overview of the GNSO policy development process or the PDP. With the Board's approval of the 2013 registrar accreditation agreement, the GNSO initiated its PDP and chartered a working group later the same year.

The policy recommendations were adopted by the GNSO Council in January 2016 and then were adopted by the ICANN Board in August 2016. After this, the Board directed the ICANN Org to implement the recommendations. Next slide, please.

And new accreditation program, as we see on the slide, actually contains more nuanced requirements than the specifications that we already discussed. And based on what you see on the screen, it is clear that the new program attempts at addressing the issues that we just discussed that are connected with the privacy proxy services.

For instance, it provides a detailed framework for provider responses to requests from law enforcement authorities and intellectual property holders, or it standardizes the requirements for providers' relay of communications from third parties to privacy and proxy service customers, and it even provides for a mandatory provider educational program.

So as we see, the new program attempts at addressing the issues with the current specification to provide for a more transparent and reasonable framework for the accreditation. Next slide, please.

As I mentioned, after the GNSO Council adopted the working group's recommendations, then the ICANN Board approved it and sent it to ICANN Org for implementation. It was expected that a new accreditation program will replace the specifications under the registrar accreditation agreement. However, currently the implementation of this program is on hold, and the reason for this stems from ICANN's efforts to bring the current data protection practices in compliance with the European Union's General Data Protection Regulation.

To go back a little bit, in July 2018, following the ICANN Board's decision to adopt the temporary specification for gTLD registration data, the GNSO Council initiated and chartered the expedited policy development process or the EPDP which is the first EPDP in ICANN's history.

Later in March 2019, the GNSO Council adopted a report, the working group's first report of the first phase of EPDP, which 27 out of 29 recommendations from this report were later approved by the ICANN Board. However, under the recommendation 27 from the phase one report, it became clear that in the view of these new developments in light of the more GDPR compliant practices in ICANN, there was need to revisit all the relevant practices that also go back—are connected to any non-publicly accessible registration data.

This is why this program is still on hold pending community feedback and review, and essentially, if we think about it, the EPDP and the accreditation program recommendations work towards the same goal, which is to determine a lawful mechanism for access to and treatment of nonpublic registration data. Next slide, please. So after the resumption of the implementation, we expect that the community feedback will be requested on the following documents. Next slide, please.

The community feedback will be requested on the privacy proxy accreditation policy, the agreement, the program applicant guide as well as the suspension, deaccreditation and transition procedures. So in short, we see that the privacy proxy services accreditation is an important issue that has worked its way through the ICANN's policy development process. But being a piece of the bigger puzzle in ICANN's efforts to have GDPR compliant practices, the implementation of the accreditation program is on hold, and in the view of EPDP recommendations, [it is essential] to harmonize the projects for all pieces of the puzzle to fit together.

In any case, the accreditation program has a more nuanced approach than the current specification requirements. However, at the same time, the underlying issues with the privacy proxy services do not seem to go away, but even as I mentioned, have been exacerbated during the pandemic. Therefore, bearing in mind the importance of the program, I hope the implementation moves forward soon enough to address the underlaying issues. Thank you very much, and I look forward to learning more on this and other topics during ICANN 72. Thank you.

DEBORAH ESCALERA: Thank you, Meri. It looks like there's a question in the chat. It says, “Could you please explain data escrow a bit in the context of the topic under discussion?”

MERI BAGHDASARYAN: Yes. It is actually a very long topic so I might just type my answer if we want to move forward with the discussion. But in a nutshell, it is about how the privacy proxy services will handle any request from either law enforcement or IP holders and how they keep and process the data that is held by these services. That'll be a short answer, but I might type a longer version in the chat if that is okay.

DEBORAH ESCALERA: Absolutely. Thank you so much. Are there any other questions for Meri? Okay, so we’ll keep an eye on the chat. Thank you so much. Very well done. Okay, so we’re going to move on to our next presenter, Sai Chandrasekaran. Sai, you have the floor.

SAI CHANDRASEKARAN: Thanks, Deborah and Siranush. This is Sai Chandrasekaran and I'm going to present on a topic today which I'm most interested about during my research, and the topic which I'm going to be talking today is about content moderation.

The topics we're going to cover today are the challenges posed by content moderation, the privacy risks which content moderation poses, and how can we resolve such a complex issue. Next slide, please.

I just want to give a quick bio about myself. I'm a graduate student of cybersecurity from Indiana University, and for the past few months, I have been working and researching on a few topics related to Internet governance, including content moderation. So I'm excited to share my views with regards to the topic on this forum. Next slide, please.

For most of you who have been tuned to the news or been plugged to social media, you might have definitely come across the buzz surrounding content moderation. So you might have seen governments trying to curb misinformation, especially in the times of pandemic, and social media companies trying to curb abuse threats and legal researchers trying to come up with some legal precedence to tackle content moderation, privacy and human rights advocacy groups raising serious concerns that content moderation poses to freedom of speech as well as privacy. Next slide, please.

I have created a brief timeline with regards to events related to content moderation. In the interest of time, I won't go through each of these events, but I would like to mention a couple of them to give a context of why this topic is relevant and how this is a very complex issue.

For example, in 2021, just a few months back, we had the US surgeon general who openly advocated to try to curb health misinformation and he told us that it poses a serious threat to public health, and limiting the spread is actually a civic and moral responsibility. In fact, [inaudible] urged the social media companies to [inaudible] to detect and prevent the spread of false information.

One thing we need to understand here is that content moderating is not a localized issue which is related only to the US. It's actually a global issue. Recently in India, India passed a series of digital media laws which required social media content providers to moderate content and to [inaudible] tracing. And this was actually met with stiff resistance from WhatsApp which filed a legal complaint in response to this new regulation.

Just a few weeks back, we had an ex-employee from Facebook giving a testimony before the senate with regards to Facebook's content optimization practices and its effects on society. Next slide, please.

So if you go and ask any person who's working in the security and privacy field, they will tell you the best way to probably solve and understand the problem is by performing a risk assessment. So I have performed a privacy risk assessment with regards to content moderation, and this is based on industry standard, industry taxonomy developed by the well-known Daniel Solove.

For example, let's assume that we are sharing information or exchanging messages through some sort of end-to-end encrypted message service like WhatsApp or Apple Messages. In that case, as a user, we have some basic expectation of privacy and confidentiality with regards to the messages being exchanged.

But let's assume that as a service provider, I use an algorithm to detect whether these messages are harmful or not, and if that's the case, [inaudible] expose this information to a tool, in that case, I'm in a way breaching users' privacy and confidentiality.

So one thing we need to understand here is going by history, whenever a new capability is being developed, we should not really think about how can we use it but we should also think about how it can be abused as well. So taking into consideration that these scanning technologies, especially in an encrypted system, can be used by government and malicious [threat actors] to probably promote surveillance and eavesdropping which has huge implications for freedom of speech in our society and creates severe chilling effect as well.

Another additional thing that I would like to let you guys know over here is sometimes, the disclosure of information can be reversed. So let's assume as a user, my intimate details such as my sexual orientations and my substance use is being exposed to the public domain. In that case, I don't have any such measures to protect from the severe emotional distress and mental effect that is being caused due to the disclosure.

Compared to, let's assume if your financial information is getting released, that's a completely different case. In that case, you can actually block your credit card as a measure to prevent any ill effects. But here in this case, since your health information is being exposed, you don't have any such [inaudible] measures. Next slide, please.

So in my previous slide, I was talking about the privacy threats which can be caused by content moderation. But on the other hand, there are some valid arguments which are being presented on the other side as well. For example, let's assume that some people say that content moderation can be used to stop violence and ultimately even prevent death, especially in terms of the violence which happened in Myanmar.

So I definitely believe we can adopt a privacy preserving approach to content moderation which is based on three key pillars. One is technical which involves collaboration between technical organizations and education institutions to collaborate and come up with secure cryptographic techniques that detect any misinformation or fake information and at the same time, they ensure their own users' privacy and confidentiality.

For example, in this case, we can use probably a secure multiparty cryptography technique which scans for images and compares that image with a repository of images which consist of all the abuse list. And if the information doesn't match, the image will not be reported to service provider.

Another important key pillar I want to talk about is process, and this is what I call an information watchdog model. So I want the users to actually responsibly disclose any sort of fake information which they are getting to the service providers so that we can generate some sort of a trust model and proactively fight against misinformation.

The final pillar which I'm going to talk about is principle, which once we establish some trust between stakeholders—let's take an example over here. If I'm a service provider who was actively moderating content, I think I need to ensure some sort of transparency with regards to my algorithms to ensure that I win the trust of all the stakeholders in the process. Next slide, please.

This brings me to my final slide, and I feel that content moderation as an issue is very similar to climate change. Different countries want to address the issue. Almost all countries want to address the issue. But they have different ways of addressing the issue. And most of the times, these things do not go hand in hand with each other.

So I would like to perform a multi-stakeholder approach to actively solve the content moderation issue with individuals responsibly disclosing any sort of fake information to the service providers with the help of the knowledge and the tools provided by the educators and education institutions. Tech platforms need to address information deficits and prioritize early detection of [super spreaders] and repeat offenders in a privacy preserving manner.

And one very key stakeholder in this process is the all the global governments together which need to convene all sort of private nonprofit organizations to find common ground or common measure for finding the appropriate legal and regulatory measures to address content moderation. So thanks for your time and patience. I'm looking forward to answering any questions you may have.

DEBORAH ESCALERA: Thank you, Sai. Are there any questions for Sai? Okay, so the interpreters had a little bit of difficulties with that one, but I want to remind everybody that this session is being recorded and so you will be able to access it in about a week or so. So if anybody wants to view this recording, you will be able to.

Okay, Enoch, you had a question? Please go ahead.

ENOCH NIKINGBOUNG DUUT: Yes. Thank you very much. A very quick question on the content moderation. Content moderation is kind of a two-sided issue. On the one hand, we don't want to impede freedom of speech and all of that. On the other hand, we also want to prevent content that should not be [in the public] domain.

So, do we have a medium point solution that mitigates the risk of allowing people to just say anything anywhere, at the same time not impeding on people’s freedom of speech? For instance, if we look at traditional media, we have regulators. But on the social media, can we have independent regulators who help in this regard? Thank you very much.

SAI CHANDRASEKARAN: Thanks, Enoch, for the question. Unfortunately, at the moment, we don’t have a readymade solution which actually provides a balance between tackling your misinformation and the freedom of speech. But I think one thing, if you’ve been watching the news recently, you would have definitely heard about the Apple client-side scanning incident.

That is with regards to they wanted to perform a client-side scanning in the user side to detect any sort of images with regards to child sexual abuse and stuff, but that has been met with civil criticism from the privacy critics and security experts as well.

So unfortunately, we don't have anything at the moment, but as I suggested in my presentation, we have something called the secure multiparty cryptography technique which actually compares those images with a repository of abuse images, and only if the information matches, it is going to report to the service provider. Else, your information would not be transmitted to the service provider. So I hope that answers your question.

ENOCH NIKINGBOUNG DUUT: Thank you. If you could put that in the chat for further [inaudible], please. Thank you.

SAI CHANDRASEKARAN: Sure, Enoch. Thank you.

DEBORAH ESCALERA: Okay. Thank you for the question. Are there any more questions for Sai? Okay, let's move to our next presenter, Kady Hammer. Kady, you have the floor.

KADY HAMMER: Hello. My name is Kady Hammer and I'm a law student at American University in D.C. I'm going to be talking about a very Gen Z term, gatekeeping, in reference to gatekeeping gateway protocols or otherwise known as security mechanisms for gateway protocols, specifically border gateway protocols. Next slide, please.

So I want to first give a brief overview of how we got here and why I'm discussing border gateway protocols. Just to let you all know, I'm not a technologist, I'm a law student. So it's taken me quite a bit of time to understand how the Internet infrastructure works. But as I'm sure you all are quite aware, the Internet was created primarily for communication purposes. Security was not necessarily a first concern or primary concern when we developed the Internet infrastructure. But it is an increasing concern in today's world, especially as we consider the ever increasing existence of cyber threats and cyber actors.

In 1989, border gateway protocol was developed as one among many protocols. BGP—which is how I'll refer to border gateway protocol going forward to be simple—relies on individual networks that continuously share information between each other about available data links, available IP addresses, which is how the Internet is able to continue its growth into the vast global network it is today.

One thing to note is that BGP does not require authentication of either IP addresses or the autonomous systems that they're interacting with. Instead, BGP operates under what's called a trust framework, or you might also know this as the honor system where the networks are trusting that the other networks are good actors.

So overall though, BGP was simple, it provided a solution to the need for routing protocols, and it provided a versatile enough structure that has lasted us through today. Next slide, please.

So here is an overview, both a diagram and a list of routing protocols. As I mentioned, BGP is one among many routing protocols. The primary purpose of a routing protocol is to route Internet traffic between other network systems, devices. One thing to note is that it does not ensure the security in the delivery of the information. So again, this goes back to the trust framework or the honor system.

As you can see, there's a long list of routing protocol types. I won't read them out to you. And the graph to the right-hand side of the screen is an overview of how BGP or another routing protocol, EGP, works. You can see how the networks talk to each other, to autonomous systems—which I will explain in a moment—and just a visual overview in case you were interested. Next slide, please.

So to get more into the specifics about border gateway protocol, BGP is a path vector routing protocol than runs between autonomous systems on the Internet. And Instead of keeping track of the Internet's entire map, BGP routers rely on information from neighbor routers or systems which then choose the route with the shortest path to include in the routing table. Each router then announce the path to other neighbors that they're seeking that information. And if the policy permits, they exchange that information.

One thin gr to consider is that when we're talking about autonomous systems or the networks that BGP is using to communicate, you might hear it being referred to as autonomous system, which implies a singular system. However, autonomous systems sometimes include a whole organization, which includes multiple routers or devices. So that term is used to speak more broadly about in more of an abstract sense.

And the Internet autonomous system numbers are assigned by an Internet service provider which is how an end user like us using Internet connects to, or sometimes it's assigned by a registry.

Ultimately, BGP helps routers choose a path, specifically the shortest path to get that information, and the reason why this protocol is so important is again, because keeping track of the entire Internet system is a feat in and of itself. It relies on neighboring networks to exchange that information so that it can get you to your information or site much more quickly.

The reason why this is important is because of the way that BGP works, systems can be targeted together. So instead of attacking a singular device, a malicious actor could attack an entire autonomous system which could include organizations, companies, etc. Next slide, please.

The thing I want to talk about today most importantly is the security issues that arise in protocols—thank you to Brian who's explaining in the chat—but specifically about the security issues that arise in BGP. Although these security issues are not specific to BGP, they do exist in other routing protocols.

One of the primary issues is a human error. We can look to the Facebook mishap which, although Facebook's issue was not entirely a BGP issue, you can look to it as an example of what could happen. So human error can create accidental misconfigurations where an entire organization or autonomous Internet system could be taken down or be missing from the Internet and wreak havoc.

But the primary thing that I want to talk about is malicious interference. So all routing protocols can be targets of attacks, whether that’s IP spoofing, session hijacking, denial of service attacks and many more different ways where basically malicious actors can introduce incorrect information into the BGP tables.

An example of that would be because BGP relies on neighboring networks, your neighboring network could be a malicious actor who introduces incorrect information in your request routing you to a malicious website or something else.

So because BGP routers trust each other, as I've noted, there are no true authentication mechanisms that exist in BGP. So there's no way to validate currently who the other or what the other network systems are saying. If the information is validated, if it’s credible, if it’s trustworthy Another thing is that cryptographic authentication isn't mandated. So that’s something else that I will get into in the next slide.

To bring this closer to home, I wanted to provide a case study on what BGP hijacking looks like and how it happened via an Amazon DNS system. In 2018, malicious actors used a BGP attack (a “man in the middle” attack) to reroute traffic to Amazon’s Route 53 service using a server at a Chicago IBX data center, allowing the actors to intercept traffic globally.

Specifically, the malicious actors targeted MyEtherWallet.com, an Ethereum blockchain platform, by redirecting their customer traffic to a fake or shell page that stole all their customers' information.

How they did this was that the Internet traffic was redirected to a server hosted in Russia, which pretended to be the webpage MyEtherWallet using a fake certificate and it stole the cryptocoins of customers. The attack required access to BGP routers of Internet service providers and required significant computing resources. That's something I want to note. Because they rerouted all that traffic, they were having to deal with the significant Internet traffic going onto their servers.

So why this matters is because this attack highlights the existing security concerns in both BGP and DNS, and more broadly into different routing protocols. To date, this is the largest known attack of its scale that combined both the fragility of BGP and DNS, which has been covered by other NextGen presenters. The infographic at the bottom is just a simplified overview of how this could occur. Next slide, please.

So, how to gatekeep. Overall, there are a few things that we need when we want to consider how to make routing protocols more secure, and specifically how to make BGP protocols more secure.

Overall, we need router software that implements IPsec, IP security. You can implement this through public-key infrastructure or digital signatures.

We need to determine the role that regional registries play in certifying authority responsibilities—so who is in charge—for address prefixes and autonomous system number, both their assignment and location.

A big component which will be a significant financial investment is upgrading hardware infrastructure including routers (ISPs and subscribers), to determine the role of ISPs in certifying and handling and certifying this information. Of course, updating physical hardware is a significant cost investment.

We need to think more strategically and thoughtfully about how we improve BGP going forward, especially, we need to keep a security minded approach going forward, hopefully with an attempt of less reactivity and more proactivity. We also need to determine the assessment criteria, so how do we determine whether or not a network, a router, any person or entity is considered a secure or validated or trusted source, what criteria are we going to use to basically allow or not allow those networks to interact and operate in the Internet ecosystem.

So the three solutions that I've put on the screen, none of them are new. Some of them actually date back to the creation of BGP in the ‘80s and early ‘90s. So there are existing solutions on how we can protect and secure border gateway protocols specifically.

One option is the secure border gateway protocol which provides three specific security mechanisms. One is public key infrastructure. This mechanism would be used to authenticate the ownership of an IP address or a block of IP addresses.

Another option in that first solution is a transitive pathway attribute. This would be used to carry digital signatures which authenticate the router information. So as that information is traveling, there's a security sort of flag in that information. Or as I've mentioned before, you can use IPsec, which is basically used to provide data which authenticates the information before any information is exchanged through BGP.

Another mechanism or solution is secure origin BGP. This actually goes back to the third point of the first solution. Before information is exchanged, each entity has to certify or be certified, so their credentials have to be validated. Each authorizing certificate must be validated. Again, this goes back to what role do the registries play, what role do Internet service providers play. Information contained in these certificates must also correlate to the larger database which would host these certificates. Again, what registry or what Internet stakeholder would play a role in maintaining such a database. And again, you have to think about the security of that database.

Another solution is called BGP scalable transport, and this replaces TCP, another routing protocol, with a proprietary transport protocol. This particular solution might not be the most feasible given that it’s privatizing this, but it would use a technique called flooding which would transport data by sending connection messages only to its neighbors instead of connecting to sort of all of the networks or all of the routers on the network. Next slide, please.

There are obviously challenges in secure border gateway protocol which is why the existing proposed solutions haven't made it through yet or why we’re still having this discussion. So the primary concern always is just the sheer cost that these solutions would require in terms of infrastructure, personnel, coordination, assigning responsibility. So those are the key components of the first two solutions.

And I've already touched on the last solution, but it requires extensive buy-in. So if you're changing a whole protocol, that’s a lot of work, and the other aspect of that is it will be proprietary, so it’s not free, and it might not be accessible, and ultimately, the authority or the controlling mechanism would go into the proprietor.

Additionally, overall, one of the most significant challenges is that there seems to be complacency or a lack of urgency until crisis strikes. I've already talked about the reactionary approach that most stakeholders—even myself included—have taken to our own security, and we tend to apply Band-Aids rather than proactive solutions.

Of course, given the longevity of the internet and how long the Internet has existed, being proactive is really difficult. And the other thing is that this problem is viewed as minor, given the small scale attacks that have happened. I did note that MyEtherWallet was the largest of its size, although it only targeted one company, but you can imagine how wide scale these attacks could occur and how much damage and havoc they could cause if BGP is one of the new focuses of malicious actors. Next slide, please.

So I've already touched on almost every bullet here, but one of the things that I want to highlight is although this is a serious concern, we can look to existing models on how we can create stakeholder buy-in and change the overall approach to securing BGP. If we looked at HTTP and how we shifted from HTTP to HTTPS, we can likely solve this issue. Next slide, please.

And that is all. Thank you very much for your time.

DEBORAH ESCALERA: Great presentation. Very interesting too. Fascinating. Okay, so there was a lot of good chat going on in the chat. Obviously, a good subject, interesting subject that people are very interested in. Are there any questions for Kady? Good job, Kady, well presented and very well structured.

Okay, so if there are no other questions—and keep in mind, you can still send questions after the session—we're going to move on to our next presenter, Scott Kim. Scott, you're up next. Thank you.

SCOTT KIM: Thank you. Hello everybody. My name is Scott Kim, I'm currently a graduate student and working as an information security practitioner. My role is to kind of collect information, analyze information, disseminate it to appropriate stakeholders. Today, I'll be talking about using ICANN lookup to find indicators of compromise. Next slide, please.

So the things that I'm going to talk about will be the summary of the APT41 threat actors, some use case studies, and then finally concluding with recommendation.

So APT41 is not well known to the community, but it is well known to the information security practitioners. APT41, also known as a different name with a different company, so they could be named Blackfly, Earth Baku, Wicked Panda. APT41 is basically a Chinese state sponsored advanced persistent threat group that conducted malware campaigns related to espionage dating back to 2012. This group has been often aligned with Chinese communist party’s objectives outlined in the 13th five-year made in China 2025 initiative. They've been known to target videogaming companies, telecommunications actors and academic sectors recently. And I shared in September the US department of Justice indicted multiple individuals linked to APT41 intrusion and operation. Next slide, please.

So recently, Blackberry research and intelligence team discovered a malware campaign conducted by this APT41 using its own customized profile to hide its network traffic. APT41 also uses different malwares like PlugX, Cobalt Strike, [inaudible], ShadowPad, and they uncovered the APT41 infrastructure by taking some of the overlapping indicators of compromise linked to two campaigns documented by two other security firms, Positive Technologies and [inaudible]. As you see in the domains, they have tried to masquerade as legitimate Microsoft domains. For the first three, the last three, five or six domains. Next slide, please.

So the ICANN registration data lookup tool gives you the ability to look up the current registration data for domain names and Internet number resources. So to perform this research, users will need to go to WHOIS.icann.org and enter any domain. Particularly for this one, I chose the isbigfish.xyz, and when I typed in the domain, this is the information that I received.

So in searching for these domains and IPs in a variety of open source intelligence repositories reveals some connections that bear further examination. The domain mentioned here belongs to 107.182.24.93 IP address, which shows up on the malware campaign blog from Positive Technologies. So they were able to connect the dots from using these open sources and finding out some of these IP addresses, domains, and what they utilize in terms of gaining access to different infrastructures and networks.

As you can see in the certificate dates, they only last about a year, which is kind of a red flag from a practitioner perspective, because usually, threat actors utilize these type of fake or parked domains for some of these malicious activities. So this will be giving us a lot of information. Next slide, please.

For the conclusion, Blackberry was able to find this information by correlating different blogs from different practitioners and security firms that was already publicly available. So this type of scenarios, we really encourage public sharing of information to kind of create the bigger picture and complete picture on a threat or threat actors. So with collective effort, we can also uncover some of the criminal activities that are ongoing right now. If you have any questions, let me know. Thank you.

DEBORAH ESCALERA: Thank you, Scott. Do we have any questions? Okay, thank you. Very well done. We have our final presenter, James Paek. James, you have the floor. Thank you.

JAMES PAEK: Thank you very much, Deborah. My name is James Paek, my topic is about digital authoritarianism, how to counter it. Next slide, please.

Pretty much a lot of you will ask yourself, what is digital authoritarianism? Based on a definition that has been provided, it is basically the use of the Internet and related digital technologies by leaders with authoritarian tendencies to decrease the trust in public institution, increase the influence of social and political control and undermine civil liberties. So anything that can be potentially an invasion of privacy, invading the public freedom and all those things that we could take for granted and may not realize that government can control over you on every aspect of [basis in] society that you can think of.

Now, I think a lot of it has to do with what are the causes of digital authoritarianism. Well, it can be the same thing as an authoritarian government, whether it can be a political, societal, economic instability, erosion of public trust on the institution, increase of legitimacy and autonomy, control and manipulate the public opinion. I think this is a common one, is the fear. Definitely, I think where we're seeing a lot of increasing public fear on what the future is going to hold in our society that we have no idea, there is a lot of uncertainty. Of course, the pandemic and all of these things that are going on right now are one of the common reasons why I think a lot of growing, increasing public distrust we're seeing here.

And of course, that includes discontent, and of course, I think we're entitled too much and we don't realize where things are coming from. And of course, I think this is very common, the nationalism, populism, a lot of political entities are starting to come into the influence, why digital authoritarianism is now becoming the norm of the reality in all the countries. Next slide, please.

So I think we're starting to see a lot of trends on this. Let's take for example in Chine which has been going on recently a lot, definitely increase in surveillance, cameras in all corners of the city within China. You can name everything, every sector, corner of the street that you go. Definitely, you're starting to see a lot of closed circuit television cameras installed on every single area that might potentially [could censor you] on every behavior that you could think of, whether it's aggressive driving, inaccurate social behavior, or whatever it is that you may think of that potentially could be deemed as an unruly behavior. And those are the things we're starting to see a lot, and that's definitely the case. We've seen in Hong Kong where China's government is starting to suppress [the Hong Kong citizens.] We saw in the extradition bill back in 2019 of course with the recent passage of China's national security law. I'm not going to go into details on that, but I would tell you the recent control revolution within China dates back to what we saw in the cultural revolution from the 1950s or in the Cold War era. We're starting to see a lot of emergence of that in China. And definitely, could this happen to other countries? It definitely can. We just don't know what's going to—and definitely we're starting to see a lot of social credit system.

Let me get into detail on this one. What is a social credit system? It's a national credit system based on the ratings of your social behavior. Like I mentioned, it can be aggressive driving, bad behavior or whatever it is that could potentially happen to you that the Chinese Communist Party may deem you as not a good social behavior. So they could punish you for whatever the reason is based on those rankings, and potentially you'll lose a lot of privileges such as going to different countries. Or potentially you might face some punishment.

Of course, we see this happened previously in South Korea as well where the national intelligence service started to blacklist Korean celebrities because of political views that they have. And starting to engage in psychological warfare from the previous government that has been seen in the past years and is starting to intimidate the Internet users. And definitely, we're seeing a lot of increase in surveillance and censorship of those who are doing anti-state activities, whatever they might deem as opposition on government policy. Next slide, please.

Other countries too, what we see right now in Russia, Belarus and France, we're starting to see a lot of surveillance and censorship. With the rigging of the election, Alexander Lukashenko in Belarus and the Internet shutdown that occurred recently. In Russia, we're starting to see election meddling and obviously interference in other countries' election. This is getting repeatedly done in other countries, which we saw a lot of rigging the election, and I think this is a really big concern on the election credibility and the election itself and the voting system. And that could potentially influence a lot of those social behaviors by basically spreading the propaganda. And we see that similarly in France, where basically, we see the national security law could give ultimate surveillance powers to the French government to monitor anyone based on the amount of harassment against law enforcement and prosecute citizens violating the law. Next slide, please.

There are a lot of different ways of what can be deemed as digital authoritarianism. Definitely, I already mentioned surveillance, censorship. That is also including electoral manipulation, police brutality, disinformation, misinformation as well as censorship. And the next slide is also in addition to that. Next slide, please.

And of course, there's a lot of it. Facial recognition, cyberattacks and hacking. A lot of this is actually considered digital authoritarianism that we actually never think of, but they're all brought into this topic of digital authoritarianism, including espionage and fake news and deepfakes, which, that is basically manipulating based on the original photo or video itself and trying to manipulate into a different format. That is becoming common right now to the point that a lot of citizens and ordinary Internet users cannot identify if it’s an original source or not and potentially, that has a lot of impact on daily society, on how we interpret it. Next slide, please.

What are the threats of rising of digital authoritarianism? That basically is very widely understood it is undermining democracy, including the institution as well as it could potentially disrupt [a lot and socioeconomic, political] and culture itself at the same time is a violation of human rights and civil liberties. Another thing—this is really not common, but this potentially could also impact women's rights, including the increase in sexual harassment or other harms to humanity. Next slide, please.

Including everything else here can be related as well as what other threats can be. And I already mentioned that all of these can be forms of what the threats of digital authoritarianism can be unintended consequences in the near future. Next slide, please.

If you see here on the recent data based on the economist intelligence unit on the democratic index, on the democracy, you see I think pretty much right now to the point we're in the pandemic and a lot of countries and governments around the world are starting to use a lot of tools and a lot of excuses on how we could actually go about and basically to proceed into the future on how we could encounter the pandemic, including how we could restore the democratic institutions and the public order.

And we see that my country, the United States, is starting to get almost into a hybrid regimes, or obviously in this case, we're in a flawed democracy. Originally, we used to score constantly on full democracies, but unfortunately, we're starting to deteriorate based on recent events which basically election and all these things going on. But if you look at the other side of the world, it's pretty much the same thing. A lot of countries have deteriorated on democracies, and that is concerning and alarming, that if we don't do anything to counter this digital authoritarianism and let the governments do the all hands on approach where basically they're going to continue to use a lot of these tools to go about our daily lives, potentially, that is harming to our society and we don’t want to see totalitarianism—North Korea or China that we’re starting to see, they're potentially going to export a lot of these, surveillance cameras, whatever it is that can be, and we need to make sure that we put an end to that. Next slide, please.

And you may ask yourself how we can counter this, a solution. There are a lot of ways, different methods. But I would say the one biggest thing that we’re going to have to do is to promote democracy, human rights at home. That’s the first priority.

And what I would want the United States to do is to lead by example, basically. If we don’t handle the domestic issues at home, potentially then we cannot set an example throughout the rest of the world and basically coerce other countries and say, “Hey, you need to follow our rights,” basically making sure that you need to uphold human rights and everything to make sure that everybody has the right to freedom, to uphold all of these freedoms.

But unfortunately, if the United States cannot do that at home and basically not willing to challenge these [inaudible] issues, then unfortunately there's no reason they could lead by example for other countries around the world. I could say this in a similar analogy where if you're on a diplomatic mission and you're representing the United States or other countries that you're representing, people are about to make an assessment or perception out of you based on your character or the person you are. That can be the similar things in here. Therefore, we need to have an increase in confidence in public institutions, including the governments.

A way to do that is to make sure we strengthen [civility] to prevent political and social [distrust.] That includes, what is common is to mitigate the racial tensions that we have in the United States and prevent division of the country. This is one of the biggest things that I really do not like, and definitely, we need to fix that in order to make sure that we need to provide units. I know that definitely is the hardest thing to do, but we have to strengthen civility in order to make sure that we have a good social character and behavior to represent, including the United States to strengthen the freedom on the Internet, digital inclusivity and accessibility. Next slide, please.

That includes a range of things. Basically, increasing the building on multilateral coalitions which we see recently with the United States [inaudible] the quad security dialog, including the five eyes, strengthening that as well. And there could be a possibility we might potentially face a possible Asian NATO into the future. We don't know yet, but [that's under trending, that potential] we see as of right now.

And a lot of public investment. Definitely, we need to invest in the human capital. I know definitely China is obviously potentially increasing investment in human capital right now, increasing in cybersecurity professionals in order to make sure that they continue to increase the talent. But in the United States, we're experiencing a lot of cybersecurity shortages. And if we don't have that or we're starting to get a lot of talent shortages on science, technology, engineering, mathematic field, we're going to be far behind and potentially, we might face undesired consequences. That includes investing in research and development. If these are not invested, it's definitely going to get far behind. And that includes a lot of different digital technologies, strengthening encryption.

At work, definitely we need to strengthen the diversity and inclusion within the workplace. Definitely, the organization [has to move forward] and go into the future, plan in order to make sure that we hire the best talent, including making sure that we overcome resilience in any national crisis, such as we've seen the pandemic that we're in right now, and a lot of things that we have to do in order to make sure that we continue to be the world's leader on technologies. Next slide, please.

Those are the references and citations. Next slide, please. That is the end of my slideshow. I thank you for listening to my presentation on these global trending topics, and I thank you for actually taking the time to listen to my presentation. Thank you very much. If you have any questions, please feel free to speak up now.

DEBORAH ESCALERA: Thank you, James. There's a question that Brian put into the chat. It was basically, I think, aimed at everybody, but since you were presenting, let's ask you. What do you think about free speech of the people on the Internet during COVID-19?

JAMES PAEK: Brian, thank you for that question. I'm not sure what type of question you're trying to ask. If I could get a clear statement on that.

DEBORAH ESCALERA: Brian, do you have any clarification on that?

JAMES PAEK: Should I wait or just say my own interpretation on that?

DEBORAH ESCALERA: You can go ahead and give your own interpretation on what he was looking for.

JAMES PAEK: I think, Brian, this can mean a lot of different things based on the interpretation [I can refer to.] But if you're thinking about what the freedom of speech of people on the Internet during COVID-19, as I said, definitely, on the presentation itself, that digital authoritarianism is on the rise. And a lot of cases that I presented, China, Russia, Belarus and a lot of these things—now, don’t get me wrong, don't expect that the United States has all the Internet freedoms and everything. Definitely, that's not true, because we definitely have a lot of work to do. And basically, we've seen in a recent case that happened in 2014 with Edward Snowden, definitely, that was an example where basically, government collected a massive amount of data because of public security and making sure that we preserve the national security after what we saw in the post-9/11 world.

Right now, as I mention that we start to see a lot of increase in authoritarian behavior controlling our society and Internet freedoms are starting to get deteriorated based on all different types of tools and techniques that we saw—like if you saw in Africa region, Nigeria where they recently had a shutdown, including other regions—I'm not sure which other African regions have been impacted. Definitely, that's basically to make sure that the government should not have the ability to control any type of freedom of information on the Internet, because what's going to happen potentially is that we'll see dire consequences. If the government is starting to control you based on what your behavior is, whatever the algorithmic data that they have that might perceive you as unruly behavior, then potentially that's something that is really concerning and the government should not have the right to actually eavesdrop on you and censor you based on what you behavior is. This is basically your freedom, your rights, your speech, and you have the right, the ability to make sure that you preserve that and to make sure that the government should not overstep the boundary. It's not their business to make sure that—they obviously should not intervene in your personal daily lives.

As I mentioned, we don't want to see another big brother years, what we saw from the previous years, including what we see in North Korea and China is also following in those steps. Do we want to see that in the rest of the world? I definitely do not want to see that. That's basically an invasion of privacy. Freedom of speech, civil liberties will get deteriorated based on that perception to the point that it is unacceptable.

I don't like obviously what we see, a lot of countries trying to do authoritarian tendencies, but I think that's something that needs to be taken care of and we need to preserve our freedom of speech and all the civil liberties, because if we don't do that, we're taking everything for granted and we cannot let that happen to make sure that—obviously, authoritarians are going to be taking control of the world. We don't want that to happen. We have to do this by making sure that we invest in ourselves and we need to increase the education, increase in public confidence in the institution.

That is difficult at this point in the United States, in the rest of the world, but we have to make sure that we actively listen, including making sure that we respect all the behaviors on other people's perception. And that's why I talked about the increase of civility, to make sure that we need to respect one another. And this is going beyond the digital authoritarianism itself, but I think the psychological aspects of why we need to make sure that we remain respectful and open and be tolerant to others whilst we have different opinions. Thank you very much.

DEBORAH ESCALERA: Okay. Thank you, James. I think Brian clarified his question in the chat. We only have a few minutes left, so I will read it to you but then I'm going to ask you to be very brief in your clarification on his question. He says, "You mentioned that government controlling people's free speech of the Internet more seriously compared to before. So, do you think that it is a good development in a democratic world?"

I'll give you just two minutes to respond to that clarification. Thanks, James.

JAMES PAEK: As I mentioned, we actually have to invest in human capital. That basically means we have to invest in our people, making sure that we increase our technological literacy. And if we don't do that, then we're going to see a lot of unintended consequences. That includes democratic developments, and that has to be making sure that we promote our democracies at home at first, and to make sure that other countries will follow along and make sure that they obviously have their own democracies as well.

[Don't even obviously think that democracy is obviously] the best thing out there in the world. I'm not saying it's bad, but I'm just saying to the point that it definitely needs to be improved. And that definitely has to be increasing in the public confidence to make sure we trust the institutions, and how we can do that is we have to make sure that we trust ourselves and make sure that we strengthen our civility at home. That's where we have to respect each other.

DEBORAH ESCALERA: Okay. Thank you. Looks like Enoch has a question, and I'm going to give you one minute to respond to that because we need to wrap it up. Enoch, what is your question?

ENOCH NIKINGBOUNG DUUT: Thank you very much. It's not a question, just an addition to the question that was asked. I think it's really important to take notice of the fact that a number of governments really took advantage of the COVID situation to pass laws that will give them the right to access or take people's digital communication exchanges and be able to use that as a reason to persecute or take action, which is kind of a higher version of content moderation.

And some of these laws didn't make news because everybody was against disinformation and false information during the COVID season, but these laws were not scheduled to end when COVID ends, so we may see governments taking these laws that were passed during COVID and taking it as an advantage to actually impede people's freedom of speech when COVID has passed. So I think it's a very important topic that we may need to consider deeper. Thank you very much.

DEBORAH ESCALERA: Thank you for your comment. Okay, with that, we are concluding our session for today. I want to thank everybody for supporting us today, for attending. Thank you to Siranush for running our slides today. Thank you to our presenters for all of your work. You did an excellent job today, very good, excellent topics and excellent job in presenting. Thank you for our meetings team for supporting us today and for our interpreters. We could not do this without you. And for everybody who attended today and supported our NextGen@ICANN 72 attendees. We're just really happy that you're here with us. And to the NextGen, enjoy ICANN 72. We have a lot planned for you this week. I know it can be overwhelming with the acronyms and everything, but just take it slow and enjoy yourself. And thank you to everybody for being here today. That's all. Have a great day.

[END OF TRANSCRIPTION]