PRAGUE – Forum on DNS Abuse
Monday, June 25, 2012 – 16:30 to 17:30
ICANN - Prague, Czech Republic

MARGIE MILAM: Hello, everyone. We are going to get started now with the Forum on DNS Abuse.

My name is Margie Milam and I am going to introduce our moderator, Ondrej Filip from the CZ.NIC who is going to be our moderator for the session and give you more information on what to expect.

Ondrej.

ONDREJ FILIP: Okay. So welcome, everyone.

I think we had a lot of very interesting talks about how to create Internet, how to build new domains and things like that, and, you know, now we should realize that the Internet is not just for the good guys but we should also keep in mind that there are some bad guys here.

So this session is going to be about the DNS abuse, one of the dark side of the Internet and of the open cyberspace. And we will have a panel discussion on this topic.

Close to my right-hand side right-hand side there are four very knowledgeable and good presence in this area, experts in this area, and we are going to have three presentations.

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.

First one will be held by Martin Peterka, the second by Branko Stamenkovic, and the third will be by two Christophers, Christopher Malone and Christopher Landi.

So the first speech will be given by Martin Peterka.

Martin is a colleague of mine. He is operating officer of the company and, more importantly, he is head of Czech national CSIRT, CSIRT.CZ so he will share some experience in this local country, how we deal with DNS abuse and what we can do about it and how we cooperate with different agencies and law enforcement and things like that.

So, Martin, please start.

MARTIN PETERKA: Good afternoon.

Thank you what you introduced me.

Okay. Today I would say a few sentences about our association, about CZ.NIC, introduce you our security teams which we operate and describe you two of interesting incidents which our team solved in the past.

At the end of my presentation, I would like to introduce you our managers, domain manager which is software which we use as our proactive tool.

So let me start with CZ.NIC.

CZ.NIC is an association. We were founded in 1998 year by 12 leading Czech ISPs. And because we have open membership, number of members grew during the years, and now we have more than 100 members.

Today we have more than 50 employees, and our core business is operating of dot CZ domain registry. Based on this role, we are part of state's critical infrastructure, and we have signed Memorandum of Understanding with Czech government which relates to withdrawal, and second Memorandum of Understanding with Czech national security agency which focused on our role in national CSIRT team of Czech Republic. I will speak about it.

We are nonprofit organization, and we have variety of other activities. For example, we have our own education center, or we have a Department CZ.NIC laboratories, which develop on software.

And of course we have security teams. Officially, in CZ.NIC we have two security teams. First of them is an internal team, CZ.NIC CSIRT, which has two main roles. First of them is incident handling within our own domain name system. Because we do not have customers, our domain name systems is, in fact, our own networks, so this role is quite simple. We really do not have incidents, so there are no problems. But the second role of our CZ.NIC-CSIRT team is much more important from our point of view because it relates to dot CZ registry.

Our team is able to deactivate domain which has harmful content. We speak about viruses, we speak about malware, we speak about phishing sites or center of botnets. And if we find the sites with harmful content, we are able to deactivate this domain for one month. And if it is necessary, we can do it repeatedly. Second security team which we operate is national CSIRT team, it's CSIRT.CZ We operate it from start of

2011 year. Till the end of 2010 team was operated by academic association CESNET based on grant with ministry of interior, which grant ended at the end of 2000 year, and CZ.NIC agreed that we will continue the operation of this team.

So we started day-by-day operation first of January 2011, and together with it we started the transfer of agenda if CESNET association.

Which transfer ended during my last year, so since June 2011 we are in full operation. Of course, we closely cooperate with colleagues from CESNET still.

Our main role is incident handling and reporting, and I believe I can say we are very successful in it, but we also do proactive steps. For example, in the second half of last year we analyzed the data from our authoritative DNS servers for the CZ.NIC domain, found unsecured DNS resolvers with static ports, and prepared the special letter which we sent to administrators of these servers with explanation of the problem. And we offered them help.

Because some of these resolvers were within governmental networks, we cooperate in this project with Czech security information service.

Our team have other activities. For example, we organize community meetings, workshops for community, and we have special courses which are focused on security in our education center.

We cooperate with international organizations, we cooperate with TERENA, with FIRST, with ENISA, and with team CYMRU, maybe you will know them, and some other.

CZ.NIC is accredited by TERENA Trusted Introducer from October 2011.

Here are some statistic of the team. You can find them at our Web page. If you are interested in it, maybe you can see what the most of incidents which we solve are from our intrusion detection system. From the rest, the most of them are phishing sites.

Now let me say something about two incidents which we solved in the past. First of them is quite new. Our CSIRT.CZ team solved it in the start of June this year and it was a DNS amplification attack.

Second one will be a little bit older. I will speak about the phishing attack which solved our CZ.NIC-CSIRT in 2010.

We'll start with DNS amplification.

Target of this attack was one of the Latvian banks, and that attack went for thousands open DNS servers from all over the world. Most of them were from United States, but a couple of thousand were in Europe and 170 of them were from Czech we public.

So our team solved this problem at the request of Latvia and CSIRT team which sent us relevant data. So we sorted them, found information about administrators and contact them, and ask them for correction.

This attack ended during a few days, as usual, but for us it's still in progress because we are still in touch with administrators and try to help them with fixing our problem.

Today, it looks about 50% of the DNS are fixed.

By the way, we were interested in nameservers which were in this attack, and we compared them with nameservers which we communicated last year in case of static ports. And so we compared with two list and we found that a few of them, five or six, were on both lists. So -- Well, anyway.

Let's go to phishing attack from 2010 year.

This attack started with complaint from one of our registrars which register a few domain to different foreign holders, to different domain name servers, et cetera, but all of them were paid by stolen credit card. It's not something what's not really usual in Czech, so we did some investigation and found that at these sites is a Trojan horse, which Trojan horse was part of attack to Internal Revenue Service, which is U.S. government organization for taxes, and the Trojan horse looked like some application which you need to run if you want to fix some mistakes in your tax application.

During next five days, we registered 150 domains which have this Trojan horse. Together with experts from IRS and registrars, our team was able to deactivate it, all these domains. And I must say, we did it very quickly. Most of them were deactivated within one hour after registration. Yes, it's quite, quite a good time.

Result was that after five days, attackers stopped registration in dot CZ registry and moved to another one, so we can say we were quite successful. But when we discussed this program, we decided that it's not enough to be prepared to incident. We need to be more proactive and try to find problems before there will be an incident.

So together with our CZ.NIC Laboratories, we prepared a special software which we called Malicious Domain Manager.

This software takes data from a few public sources which are focused to store data about malware and phishing and other harmful content. We use Malwarepatrol, Phishtank, Zeus Tracker and a few other sources to this application. So we take this data, select from them sites and sources within dot CZ domain, and search contact data for these domains. And because our application is connected with a ticket system, our experts are able to communicate with these administrators and contacts and check if they repaired the sites, if they fixed the problems.

We started this application last June, so now it -- now it's running for one year, and here are some results. During this one year we are very proud that we helped with cleaning of more than 11,000 pages, which were in more than 2,000 domains.

At this chart, you can see data from Phishtank where are percentage of phishing pages within dot CZ between June and December 2011. You can see that there is a big drop, from 6% in June to 2% in December.

This chart doesn't continue because Phishtank shows only data about countries which are above 2%. So I'm pretty sure it wasn't only because of our Malicious Domain Manager, but I believe we helped them.

This application is open source, so if you are interested to download and use it, you can do it. At this slide is a link to this project.

Thank you for attention.

ONDREJ FILIP: Thank you very much, Martin.

Well done, indeed. It was a presentation from the ccTLD registry. We will not take any question directly after the presentation. There will be time after all of them are finished.

So without wasting time, I would like to ask the next speaker, Branko Stamenkovic, to deliver his presentation. Reading his bio would probably take another presentation so I will not read it all. He has been involved in many cybercrime projects, either nationally in Serbia, at European level, or internationally, and his affiliation is head of Special Public Prosecutor's Office for high-tech crime of Serbia.

So, Branko, please.

BRANKO STAMENKOVIC: Thank you, Chair, very much.

Let me just see -- Okay.

So -- Yeah.

As Chair was -- as Chair said, my name is Branko Stamenkovic. I am the head of the Special Prosecutor's Office for cybercrime of -- Sorry. It is on? It should be on, yeah. Sound better, I believe. Okay. Thank you.

So my name is Branko Stamenkovic. I am the head of the special prosecutor's office for cybercrime of Serbia. And, yes, I am government and even worse, I am part of the criminal justice government. And I believe that this first time which is going to be for me this ICANN meeting for which I have to thank Margie and good people from the ICANN. You are going to be, let's say, benevolent to me because at this moment I have to share in my presentation let's say three levels of what at this moment is going on when it comes to the tackling of the cybercrime in the world, on the local level and then in the third part, some of the indications which we encounter in Serbia.

So on the global level, we have one tool when it comes to the tackling of the cybercrime, and it's only tool at this moment and that's the Cybercrime Convention of the Council of Europe, see ETS 185, or popularly called Budapest Convention, which was signed and open for the signatures in 2001. And so far, 47 states from all over the world signed or ratified this convention, with the prospect of many more joining the cybercrime convention.

What's very interesting about this convention is that it belongs to the Council of Europe as the organization of the European states, but it's open for the ratification and, before that, signatory by all the countries all the around the world.

As you can see, Serbia ratified that convention in 2005 -- signed in 2005, ratified in 2009 and put into force as well in 2009. United States signed in 2001, ratified in 2006, and put into the force in 2007.

This tool brings, let's say, the U.S. authorities and let's say Serbian authorities in one joint force for committing cybercrime all over the world.

Summary of the treaty. The convention is the first international treaty on crimes committed via the Internet and other computer networks dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

You can see on the screen that the cyberspace criminal conducts which are envisaged by the cybercrime convention are divided in four groups.

First is offenses against the confidentiality, integrity and availability of computer data and systems. Then computer-related forgery and fraud. Then content-related offenses such as child pornography, xenophobia, and racism.

And fourth, offenses related to intellectual property rights and similar rights plus the combination of offenses such as spam, phishing, ID theft, botnets, terrorist use of ICT, and so forth and so on.

When it come to the offenses against the confidentiality, integrity and availability of computer data and systems, which in a broader sense DNS abuse falls to, there is the legal access to computer system, legal interception, data interference, system interference, and misuse of devices.

And in the scope, the Budapest Convention tools are in the criminalizing conduct, meaning the substantive law, as illegal access, criminal acts of illegal access, illegal interception, data interference, system interference, misuse of devices, fraud and forgery, child pornography, and IPR offenses. And then we have the procedural tools which are the expedited preservation, search and seizure, and interception of the computer data.

So every country which signed or ratified on the end this convention has to have within the local legal framework, legal framework of that country, all those substantive and procedural law tools embedded into the law system, which at the end of the day will make all the criminal authorities, criminal detecting authorities when it comes to the cybercrime in the world on the same page and with the same tools, easing us of our line of the work when it comes to detecting cybercrime.

Then on the local level, we have the Serbian example which started back in the '90s, and one of the very important tasks which we had in front of us was on the national level.

So fortunately enough, the government of the Republic of Serbia and the Ministry for the Digital Agenda, during 2010 and 2011, adopted the national strategy for the development of the information society, which is the key text, key document, when it comes to the organization of the protection of the Internet and cyberspace when it comes to Serbia on the level of the state.

As you can see, national strategy for the development included to gain the trust of the citizens and other users in the secure functioning of the ICT systems and security of the personal data in those systems, an awareness widening about necessity of using the information security measures, protection of the data, and so forth and so on.

What is, let's say, specific about my country is that in the very early stage, we understood the necessity to have the specialized government authorities for combating cybercrime, and at this moment, even on the level of the European Union, that kind of specialization is rather rare.

One of the reasons why this specialization happened in my country is that the scope and the load of the -- let's say the cybercrimes was very high during the '90s and in the beginning of the 2000s, and of course one great, let's say, ignorance of the judicial prosecution and police system in my country led to believe that only the specialized government authorities could spearhead or could tackle this new challenge, this new threat, and put it into the cybercrime -- cybercrimes which were affecting Serbia and affecting the world from Serbia by the Serbian criminals.

So as you can see, the very idea began into the late '90s and during the 2000s.

In 2004, the draft law was made. It proposed the -- then proposed to the National Assembly.

In 2005, the law was empowered, was adopted by the National Assembly.

And from 2005 onwards until these days, we have the special law on the organization and competence of special government authorities for combating cybercrime in Serbia.

That law includes organization. It's procedural law and organizational law; it's not substantive law. And it includes, in the first place, organization on three levels of the government authorities. First of all, there is a special service within the Ministry of Interior, then the special prosecutor's office, and then the special chambers or special court for the cybercrime within the higher court in Belgrade.

Of course together with those government authorities, we are now on the beginning of the, let's say, forming of the national SIRTs. At this moment we only have the academic SIRT in Serbia, not the governmental one, so I hope that in the time to come, in the very near time to come we are going to have this important body as well meeting the system of protection against cybercrime in Serbia.

Just briefly to go through the substantial law, as you can see we have three groups of the criminal acts which are different by the way of the execution and on the way of the -- how the, let's say, criminals are acting when they're executing these criminal acts.

And all -- I have to underline that all of those criminal acts are completely in the line with the Budapest Convention.

As I already mentioned, we have the special prosecutor's office. Then we have the special service for the suppression of cybercrime within the Ministry of Interior. And then we have the organization and competence of the courts. As I already mentioned, the specialized chamber of judges within the higher court in Belgrade is handling those cases.

You can briefly see the statistical data for the special public prosecution office for combating cybercrime. At this moment, we have over 2,600 cases within, let's say, our portfolio.

Now, something about the cases. And yes, the mask is there. The famous mask.

This case is rather new and this is the first case in which we encountered the Anonymous organization, let's say, in Serbia, which brought to our attention by the defacing and trying to get into the depth of some of the government servers, defacing of the namely minister of justice, the republic prosecutor's office, and not only that, but some other government authorities' Web sites occurred.

Some of the, let's say, false DNSing and some of the proxying, which were being used by the Anonymous proxy was used, and on the end of the day, when the search and seizure of the premises of the -- at the moment, the suspect and later the accused one was conducted, we realized that during only, let's say, six months -- the last six months of his acts, he managed to have six -- 776,590 PHP shells seeded all over the world and in Serbia as well. What was very interesting is that only one guy -- only one guy, with a bit of the help from another guy, succeeded in penetrating at that moment in, let's say, 50% of the Serbian ISPs, and he took control of the route servers of those ISPs, meaning effectively that he was able to control (audio problem) on the root servers of some of the major ISPs in Serbia.

One of the big threats in Serbia as well is the abuse of the credit cards, and that abuse of the credit cards is, of course, always coming with the false identities and with stolen identities on the Internet, and by the use of the credit cards with the Anonymous proxies all over the world but some of those proxies were discovered in Serbia as well.

So on the end of the execution of these criminal acts, you have always a citizen or a company, but in our case it's mostly the citizens which are experiencing the lack of their property on their credit cards or on their debit cards. So one can imagine that this kind of the execution, the criminal acts, is -- is very much of the danger for the, let's say, a simple man or the small man.

One of the criminal cases which we encountered as well is, of course, the Internet child pornography, and Internet child pornography, by the definition, is always using -- the perpetrators of those criminal acts are always using the false DNSs, the anonymous proxies, the servers on the undernet or any other branch of the Internet which is not that much in the, let's say, controllable space by the ISPs or by the government. So when we are going for those criminal perpetrators, we have to arm ourselves with a lot of patience and a lot of knowledge and a lot of international cooperation.

At some moments, we encountered, well, not that good cooperation by the foreign ISPs and the foreign authorities when it comes to the tackling of this particular problem, but I have to admit that we have impeccable cooperation with the U.S. authorities when it comes to these problematics. And I believe that the -- let's say the danger of the Internet child pornography which is present today in the world will wake up all those who are still sleeping in this area.

This is one interesting case about the abuse of the Internet domain, which was the EscrowEurope.com.

The false DNS and the false site was put on by the perpetrators from Serbia, which basically asked for the escrow from the boards -- online boards in the U.S. which were set up for the escrow or trade of the vintage electric guitars or vintage items, and then when that kind of the execution went well for them, they even accelerated their conduct and you are going to see now some of the items which they acquired with execution of the criminal act over the Internet.

On the left side, you can see those vintage guitars ranging from $2,500 all the way up to $20,000, and even on the end of this action, we will -- we were able to seize Kawasaki Ninja racing bikes, so this is very interesting.

So this is just to -- to picture in this world and in this moment what the perpetrators of the criminal acts are ready to do in the -- in the course of the execution of the criminal act and in order to get the financial gain.

Even to transfer that motorbike from Oregon to Belgrade using the cargo plane.

And, yes, always the DDOS attacks which are very often and which can get -- and which can inflict very, very high damage, not only to the ISPs but to the -- all the users of the ISPs. Namely, the companies. And, yes, on the end of the day, the citizens or the populations of some country.

For example, this particular DDOS attack which happened in Serbia shut out the very core of the Internet access in Serbia for 12 hours.

So the main backbone of the communication between the providers from the -- outside of Serbia and main Serbian provider at that time was in jeopardy, and as I said, for 12 hours we weren't able to have none of the traffic coming into Serbia or going out.

So in a nutshell, yes, I am the member of the government and yes, I'm part of the criminal justice system, but as you can saw in my presentation, the specialization of the government authorities is a trend today, and you are going to more and more see the specialized police officers, specialized legal enforcement agencies, but not only them, because they are out there for, let's say, 10 to 15 years at this moment, but you're going to see more specialized prosecutors. You're going to see much more specialized judges, which are going to be the ones which are going to file subpoenas, which are going to ask for additional informations, and yes, which are going to go transborder. We are not going to just stay within the borders of our countries because the cybercrime is a transnational crime, it's a transborder crime, and we are going to use the tools which are in our possession, such as the Budapest Convention of the Council of Europe, and ask for the information and ask for the evidence, and we are going to do that in the cooperation with our colleagues from the legal enforcement agencies, public prosecutions, and so forth and so on.

Hopefully with one good goal, and that is the protection not only of our societies, but the society of the world as well.

Thank you and I am going to wait for the questions on the end. Thank you.

ONDREJ FILIP: Thank you very much, Branko, for your presentation.

Another presentation will be more about investigation methodology and domain name seizures and they'll be delivered by two officials from the U.S. Government of Homeland Security -- I think it's homeland security -- Investigation Cybercrime Centers. And first is called Christopher Malone. He's closer to me. And the next gentleman named Christopher Landi.

So gentlemen, please start your presentation.

CHRISTOPHER MALONE: Yes. Thank you, Chair, and thank you, Margie, for the opportunity to present today. It's very much appreciated.

As mentioned, my name is Chris Malone. I am a special agent with the Department of Homeland Security's Homeland Security Investigations, and I'm assigned to our cybercrime center in Washington, D.C., what we call C3.

And myself, in concert with my colleague, who will introduce himself, are members of the ad hoc law enforcement advisory group to the GAC and, as many in the room will know, have advocated to that body on a number of law enforcement interest Internet governance matters -- I would say public safety matters, not just law enforcement -- regarding concerns of the type of the IPv6 transition, standardized record retention periods and accuracy of those records. But primarily what I'll tell you what speak to here and has been discussed over the past 48 hours is accuracy and the importance of WHOIS data to our investigative activities.

And in our capacity, in discussions with that group, members of which are present here -- the FBI, DEA, Secret Service from my own country and our foreign colleagues, SOCA and those in the U.K., colleagues in the RCMP, and Europe -- we share a vision of the accuracy of this data, of the WHOIS data, and its importance to our investigative activities.

And in my interaction with them, we've discussed that frequently we perhaps take for granted a presumption that people understand and can intimate how we conduct our investigative activities, which seem quite obvious to us, but in thinking through this process, we're aware that sometimes folks may not know the methodologies we use to initiate and conduct cyber-based investigations.

So in the light of that, I have a brief presentation touching on what may even appear to be somewhat of a mundane nature which we initiate and conduct these investigations, to give you some perspective of the importance of the accuracy of that data to initiating our -- some of our activities.

And I speak today advocating for the investigator in the field, the criminal investigator conducting his field activities, versus from a policy standpoint or advocating. Although we do advocate good government and good public policy with regards to these issues, I'm advocating for the conduct of the agents in the field.

So to give some clarity into the value of this -- the accurate -- accuracy of this data, an agent in our organization comes into possession of IP address information through any of a variety of means. It may be an IP address associated with some type of illicit content being hosted on a Web site such as child exploitation content on a Web site. It may be IP address data associated with the exchange of e-mails. E-mails potentially revealing criminal activity.

Regardless of how this what we would describe as dirty IP information is coming into possession by the agent, initiating response is to go to those open source resources and track down, potentially, a record holder, an ISP, that can point towards a subscriber for that -- in the process of identifying that offender.

So they're going to the domain tools, they're going to WHOIS, they're going to the ARIN Web site, they're using open source tools and methodologies to connect to -- hopefully connect to an ISP.

That agent will seek to generate a subpoena through various legal processes. One primary would be as issued under a grand jury -- a grand jury investigation in my country. Obtains that grand jury subpoena, potentially, to go to that record holder to obtain subscriber information, perhaps obtain log-on and log-off information to obtain additional IP addresses and track the location of that offender.

It's important to note here that we're not talking about the expansion of tools or authorities. These tools and authorities are already in place, and in discussion with my foreign colleagues, in the majority of instances they likewise have similar tools and authorities. And I advocate for certain expansions of some of these authorities, but what we discuss here is not an expansion of any type. These are legal processes which are under judicial scrutiny within the U.S. They are not at the discretion of the investigator, if you will. And ultimately, at some point in the investigative process, at the end of that road, are subject even to scrutiny of our -- the prosecutors to whom we bring the cases, judges and magistrates, and ultimately potentially 12 members of our peer group in the form of a jury.

So these are not tools either unique to this type of investigation, nor are they seeking to request an expansion of these tools.

What we talk about as this initiating step for the agent in the field is critical in being able to accurately get those records, and I can tell you that anecdotally, when these subpoenas are generated, a service provider cannot be expected, obviously, to act instantly. They're entitled to a reasonable amount of time to make that response. 14 to 30 days is a common response period.

Inaccurate data, at the end of that 30-day window, as you can imagine, with a nonresponse for a service provider, leads to the generation of a new request to a new ISP because -- because of the either nonresponse, the nonretention or nonaccuracy of data which is transferred en bloc, so the -- as you can imagine, the more of these roadblocks that are hit, the expansion of this -- this time period takes place.

This cyber-based data, as you may know, is perishable. There are not standardized record retention periods. There's discussion of legislation in my country. I'm aware that there's discussion of such legislation in other countries. Notably my RCMP colleagues would speak to what's going on in their country with regards to that.

But the -- any delay in obtaining that information accurately obviously delays the investigation itself.

I also want to point to this slide with reference to some other investigative techniques.

The obtaining under lawful judicial process of subscriber information, subject to a request from an ISP, is not -- the accurate IP address is not a panacea. Obtaining this information does not lead instantly to your target violator.

This is an initiating step, in many instances, to an investigation which requires all the other investigative tools that we can bring to bear. Agents are still obligated to connect the person paying those bills with the online activity, potentially. The person paying those bills may not be the offender or violator. There are a whole host of other investigative steps which are intimated to here on this slide. The due diligence of the agent will lead to hopefully identifying the target individual and obtaining the digital evidence and other evidence, frankly, that leads to the successful prosecution.

So this is we're often perceived as running some nefarious large database enterprise of trolling this data. This is frequently an initiating step. Can be a verifying step. It can frequently be a dead end or lead to additional and -- expansive additional research that needs to be done. So that's one of the things we want to clarify and give some perspective, that frequently we hear government's resources must be unlimited on these issues. I advocate for the manage in the field managing 5, 10, 20 cases who has to take these initiating steps, the more interventions complicating his successful investigation of, let's say, potentially a child exploitation crime online and the possibility of that evidence. And the extended periods that we have to permit to allow accurate response from ISPs necessitate the accuracy of this WHOIS data.

And so having said that, I'm going to -- chair, if you will permit, I pass directly to my colleague to complete the presentation.

CHRISTOPHER LANDI: Good evening, everyone. as Ondrej mentioned, my name is Christopher Landi. I work at the Homeland Security Investigations Cybercrimes Center. First, I would like to congratulate my colleague on using the word "panacea" in a sentence. I was quite impressed.

What I'm going to discuss briefly is what happens after we identify an abused domain, whether that's a domain that's hosting child pornography images or intellectual property rights violations. What's one of the tools -- other than the obvious of going and putting handcuffs on the individuals, what's one of the tools that we can use to get the offending information off the Internet? And that's domain name seizures, actually seizing the domain name through legal process.

Sounds scary but it is something that we actually go through and take very seriously, and we have some safeguards in place.

So what we would like to do, as the slide states, we implement these seizures to make sure no legitimate activity is disrupted. What we are going after here are the really bad actors, the people who are hosting child exploitation material in one case, we found that had images of 2-month-old children being molested. That's what we're going after.

So one of the first steps we do in that is we want to identify the full URL. We want to make sure that all the little characters, all the typos, everything is exact because we know on the Internet how easy it is to make one little typo and you get a completely different result. That's step one.

We also want to know exactly where that illegal content is being hosted, so it could be hosted at a third level, a subfolder. Where is that illegal content? And if it's hosted on a subfolder, where's that hosted within that subfolder?

So then we're going to verify the content. Now, we could get information on the URL from a private citizen, from another law enforcement agency, from one of the record holders.

The first step we do is verify that content. Is that child exploitation or IPR material still there? Has it changed? Capture the contents of the Web site so this way we know for law purposes, for legal purposes, down the road exactly what it was at the time we captured it.

Then we identify the listed registrant of that Web site. This is where that information becomes very important because if we can't determine who owns that Web site, who the registrant is of that Web site, it delays the investigation. In some cases, it means that children victims are being put online. In one case, it was actual live images of children being molested.

We can't take that Web site down. We can't find out who the perpetrators of those crimes. Once we are able to identify that, we identify and we verify the hosted content at the URL. We also identify any legitimate activity. So we're looking at where's the illegal content; where, if any, is there legitimate content which has happened in cases. Now, if there is no legitimate activity and, say, for instance, it is all child exploitation material, what we will do is we will apply through a legal process to shut that Web site down. We will not just call the record holder and say you need to shut down this domain name. That doesn't happen.

We might notify the record holder. We might notify them that there is illegal content, but we will always go through the judicial process to get the appropriate, legal paperwork to shut that Web site down.

This just goes into a little bit more about if it's hosted in different locations. But the important thing to know and what I would like to make sure everybody understands is we are not going after or shutting down Web sites of people who are having, say, one copyrighted image on their Web site. We might go after somebody who is making millions, if not billions, of dollars hosting hundreds of thousands of images or the child pornographer manufacturer, the distributors of child pornography, the producers, those are the Web sites we are shutting down. Those are the people we are interested in.

With that, I will turn it back over to Ondrej.

ONDREJ FILIP: Thank you very much, gentlemen, for the interesting presentation. So now here's the moment where you, ladies and gentlemen, can ask some questions. Are there any questions? Excellent. There are.

Please state your name and affiliation when you are asking.

FRANK SCHILLING: My name is Frank Schilling. I'm the applicant known as Uniregistry, I guess, a registrant of domain names, SLDs and a registry -- future hopeful registry operator. I actually came for the next session, but I was listening to you guys, the end of your session here. And it was really interesting.

I think as an Internet consumer and registrar, registry operator -- would-be registry operator, the risk is, we are all moving towards this post-9/11 "V for Vendetta" world where, you know, things used to be a certain way where there was, you know, due process and there was -- you know, there was this -- sort of this -- government was there to protect us.

The risk is that we're moving to this world where, you know, while your intentions as law enforcement are well-meaning, that we overreach, we overstep, we make mistakes. You read about it in Drudge three times a month and that these mistakes happen. and we get to this unholy place where the pendulum overswings.

While your intentions are certainly pure and respectable, none of us want to see child pornography, really, clearly. None of us want to see laws being broken.

As you become judge, jury, and executioner -- or maybe even a better analogy if you remember the film "Judge Dread," where we have an instant law enforcement, the scene comes up, the judge is there and then in 30 seconds a judgment is made, and punishment is carried out.

While some of this may be a natural evolution of technology, you know, some of it makes us who remember the world pre-Internet, it makes us bristle with nervousness. You know what I mean?

Can you guys speak -- the two gentlemen on the end, can you guys speak to -- do you have any sort of internal discussions about, Hey, are we going too far here? What about this? Rather than the embarrassment that might be caused by a Drudge-like mistake that gets made and everything gets taken down by accident.

Do you guys have any kind of internal checks and balances that you guys are -- or anything that you can speak of? When we do things in our business, we kind of think about what kind of countermeasures are we offering, equal and opposite reaction to our action. Do we check and balance? If you read between the lines to that question and just speak to some of that.

CHRISTOPHER LANDI: Sure, I can answer your question. There are certainly checks and balances. I by myself could not go down and take a domain. I couldn't complete an entire investigation by myself. That is certain levels. You will have the agents in the field. You will have multiple agents working the case. You will have supervisors. You will have first-line supervision, second-line supervision.

We then take that case to a U.S. attorney or local prosecutor. They're reviewing it. A judge is going to review it. There are a lot of those checks and balances in place.

I understand what you are saying about is there an overreach or does the government sometimes go too far. For fear of getting my wrist slapped, I won't answer that question.

But what I can tell you is that the reason that law enforcement does attend these meetings is because we look to the community to actually come up with a lot more of the answers than we can. So we're not looking -- the members here at least, we're not looking to, say, legislate or ram anything down anybody's throat.

What we are looking for is, hey, here is our issue. Here are some of the type of things we are looking at. As a community, as the technical (audio problem) managing the Internet, how do we solve this? How do we allow the Internet to continue as free as it is without having these bad actors, so to speak, out there ruining it for everybody. Because it is a small percentage. Sadly, though, how many children being molested is okay? So that's the question.

FRANK SCHILLING: Nobody has a good answer for that, clearly, right? That's the unthinkable. Nobody wants to think in that way. That gives everybody, law enforcement, huge latitude.

You spoke very eloquently just now about that you have checks and balances and supervisors but, yet, three times a month -- not recently but every month we hear about an overreach that does slip by.

We're just -- you know, it is not you guys specifically. But it is just the system that we're sort of cultivating as we all kind of sleep walk into this. How far is too far? And if there is nobody speaking to the point that, Hey, we've overswung here, we've gone too far, then we get to an unhealthy place on the other side of that pasture which has the risk of shifting power away from the U.S. and foreign registries, which we don't want.

I'm a U.S.-centric guy. I'm not an American. I don't live in America. I am a U.S.-centric guy. I grew up on American television. I love America.

But I think there is a risk with this constant overstep that if you take it to its logical conclusion that we get to a point where we you kind of swing the balance of power away from a U.S.-centric environment.

And that's just sort of something that keeps me up at night. In the back of my mind, if we keep going down this path, you almost need a check and balance somehow. I'm not myself sure of what that is. I guess that's why we attend these meetings, to talk about it and find it.

CHRISTOPHER MALONE: Sorry. Just to amplify some of what is being discussed, you mentioned checks and balances. Just very briefly, the ultimate check and balance is that your criminal investigators are the instruments of a lawful judiciary in whatever country or government that their conduct is represented.

So, for example, in my instance, one of the prosecutors within my jurisdiction and venue is present in the room.

I don't know where you are, Peter.

But he is an ultimate check and balance. And he is not going to bring to trial a case that I bring to him that he can't defend. And he is not going to bring to a magistrate or a judge a case he can't win. It is not -- the ultimate arbiter is a jury of 12. These are the extensions down the road of what you are discussing.

We are not talking about the conduct of nefarious or nebulous intelligence activities. These are lawful investigations using approved and honored judicial tools to obtain this type of information and they are under scrutiny in a number of layers to include at the most base level, which is an investigator is not going to go seeking stuff that's not relevant or germane to his investigation. Doesn't, frankly, have the time to give up that type of thing.

As Chris intimated, we're targeting large networks of activity. So that in itself is a check and balance of the time of the government and it is worth to expand on that type of investigation.

NANCY LUPIANO: Margie, I'm terribly sorry. We are coming near the end of this session.

MARGIE MILAM: Do we have enough time to finish the queue in?

NANCY LUPIANO: Five minutes at the most, please.

ELLIOT NOSS: Elliot Noss with Tucows.

I want to speak a little bit about language in this dialogue.

Christopher, you referenced "child pornography," I counted five times and you referenced "intellectual property" issues one time. And when you did that, you said "but these are not single images. These are people who make millions or billions of dollars."

I would really challenge you to identify a single violator of intellectual property that's been taken down around a domain seizure that has ever come close to billions of dollars.

The reason that I call out this language is because the public data that's available suggests that the majority to the -- the vast majority of these domain seizures do relate to intellectual property issues. And the expansion of the criminalizing of intellectual property issues has really exploded in the United States in the last three, four, five years.

So when we're talking about these issues, I think it's more credible to -- you know, there is nobody in the room who is in favor of child pornography. We can take a straw poll. We're not going to get there.

But there are much more controversial issues around the expansion and the criminalization of intellectual property rights. And that's where a lot of the pushback to these issues comes from.

And we see today currently -- there is an extradition of a 22-year-old kid in the United Kingdom where now we not only have an expansion of the criminalization of them in one country but an extraterritorial application of those laws. And it is these things that scare a significant portion, not just of the ICANN community, but of the Internet user community.

And, you know, I would really suggest to you -- because, you know, we will line up arm in arm when it comes to child pornography and a number of other issues that are very serious crimes that are dealt with domain seizures; that you would be able to get so much further down that road, so much greater expansion of rights and so much more cooperation if there was some way to potentially sever some of what I'll certainly call the more serious, clearly indisputably criminal issues and some of the issues that a significant portion of the population sees really as enforcement of private commercial rights. Thank you.

[Applause]

CHRISTOPHER LANDI: And I appreciate your comments. And I believe IPR is more of a legislative issue. I can't speak to my agency's policy and whether I agree or disagree. But one thing I can say is we do have financial crimes that do run in the billions of dollars. Are they linked to IPR? In some cases, there is some leadover from IPR violations. Is that the only one, say, that corporation is involved in? No, it may not be the only one that criminal organization is involved with but it does run into the billions of dollars. We do investigate those types of crimes.

As far as IPR and getting, say, on board with -- or, yeah, it is easy, child exploitation is the easier of the two of them, like I said, to me that's more of a political investigative issue. The public has the power there in what laws they want enforced, what laws that they want changed. So I don't see too many people lobbying for, yes, you know, We want to be allowed to molest 2-month-olds. No, nobody is pushing for that.

As far as IPR violations, yes, I understand there is more of a conflict. And I understand that and I understand what you're saying.

ZAHID JAMIL: Thank you.

ONDREJ FILIP: Just a very brief question.

ZAHID JAMIL: One minute. People usually say I speak too fast because the scribes have problems. But just wanted to make a point in IPR -- Zahid from the GNSO Council but speaking in his personal capacity, just for the scribes. I come from a part of the world, from the (indiscernible), et cetera, where IPR is actually something that feeds organized crime as well.

So maybe in the U.S. case there is a lot of other sort of stuff. But I come from a part of the world where we see a lot of that sort of stuff. To that extent, I would support some of the work that you're doing.

Talking about a U.S.-centric or otherwise approach, it seems to me the problem is really that the rest of the world hasn't really come up to the level of certain -- some sort of enforcement when it comes to -- on the Internet.

I'm thinking by way of what Branko said about the cybercrime convention and how that can help and to what extent do you see that as a global as opposed to simply a regional. A lot of people say it is regional. It seems odd to me I don't see the U.S., Canada and the European Union in one region. I don't know, it seems odd. And Japan.

So to what extent do you see that as a global tool and a global convention? And with respect to allowing consensual disclosures by private parties to law enforcement agencies cross-border, have you found transborder access, which is in the convention, useful? That's pretty much it. Thank you.

Oh, one other thing. Can we get copies of these presentations because they are not on the Web site right now?

MARGIE MILAM: They will be posted. They should be right now. But, unfortunately, I think we're out of time. Can you quickly --

BRANKO STAMENKOVIC: Yes, I see the Cybercrime Convention of the Council of Europe as the global tool because it was endorsed by, let's say, all members of the Council of Europe together with the U.S. As you mentioned, Japan is on the way to ratifying the convention. In the last October's conference, which was just in a few weeks ago, we -- as the Council of Europe, we acknowledge many countries from South America and from the Far East as well ready to implement the cybercrime convention and to ratify. If not ready to ratify at this moment, many other countries led by the provisions of the Budapest Convention put the legal tools envisaged by the cybercrime convention into their local framework -- legal framework.

So, yes, it is a great tool, directly or indirectly, and I would like to see more and more countries to lead to the process to the success of the convention. I will close with that.

ONDREJ FILIP: I'm afraid we have to stop right there. It is a very interesting discussion, but we do stop at this point. Thank you very much all the speakers for this very lively discussion. And special thanks for Margie organizing this very interesting session. Thank you very much.

[Applause]

[End of Transcript]