Transcription ALAC Policy Meeting 23 June 2009 – Sydney

Evan[?]: For a very few minutes before we start the next meeting, I just wanted to introduce you to something that we're considering.

I would like you to check your e-mail for something sent to the internal list that was sent by Patrick last night. It is about the possibility of doing a join NCUC ALAC commentary on the IRT, here at this meeting.

This is not just simply a document. It's an intention to actually have a strategy that has as many bodies up at the microphone at the public forum as possible. So there's an intention of trying out a strategy of making it clear to the board and to the rest of the community that the user constituencies of ICANN are very, very much against the fundamental principles of the assumptions made in the IRT -- as well as most of its conclusions.

We will be addressing this in more detail later. Cathy's here from NCUC. Basically, she, Patrick and I have been involved in trying to wordsmith something to be said at the public forum -- to complement the statements that, as you know, Patrick has made. And other statements that the NCUC itself is going to make.

So we are going to be tackling this later. Cathy -- do you have something to add?

Cathy: Thank you for the invitation to join you.

V: [inaudible]

Cathy: [laughter] I really enjoyed being at the meeting yesterday.

V: [inaudible]

Cathy: I've been with ICANN since the beginning. My first meetings were in 1998 in Berlin, in 1999 in Santiago. In 1999, the UDRP was introduced. It had no rights for registrants -- no rights for domain-name registrants -- no rights for individual registrants, non-commercial or commercial registrants.

The only way we stopped it was by putting lots and lots of people up at the microphone. The press happened to be covering it, and we said, "Look. There are rights of freedom of expression involved, here. The rights of fair use. You need to consider those. You must stop this process until you take into account the concerns of everyone in the Internet community."

So I'd love to urge everyone to pick an issue on the IRT report. The IRT report was written entirely by the world's largest trademark attorneys. The trademark attorneys that represent the largest brands in the world.

There's real concern about what the implications of the report are for speech. And for the use of words. And for the use of the future of domain-name registration.

So we've drafted a very short joint statement. But I know that Patrick and Evan have done wonderful work with comments on the IRT report. The non-commercial-user's constituency. I have to run, because I have to go back. We're also submitting lengthy comments.

But if we can do something short together… Also, if every person in this room got up to the microphone and said one element of their concern with the IRT report, the board would notice.

They'd have to! You'd be up there for 25 minutes or more, making them listen to your concerns. You're much bigger than the NCUC. You have the ability to really capture the attention.

Do we have the schedule in front of us?

There are two times when public participation would be very important. Evan -- do you have that in front?

V: I believe that we have a…

Evan: Yes. Actually -- okay.

V: We can [inaudible]

V: [inaudible]

V: Okay. Two opportunities will be Wednesday afternoon at gTLD -- the new gTLD forum on trademark abuse. And Thursday morning at the public forum [inaudible]

Cathy: Thank you.

V: [inaudible]

FV[?]: Thank you, Evan. Dave -- sorry for this delay. But we are less than…

Dave: Thank you for having me here, today. My name is Dave Piscitello. I am ICANN Senior Security Technologist.

Many of you know me as being a participant in the Security and Stability Advisory Committee. Another hat that I wear at ICANN is that I work with the security staff on global operational responses -- on issues that are brought to ICANN that have security, stability and resiliency concerns at the top level and root level of the DNS.

I'm here today to talk to you about something that I believe many of you may be familiar with -- which is a very, very long initiative to combat and contain a fairly nefarious Internet worm and botnet called Conflickr.

The presentation that you're about to see is being given to many of the SOs and ACs. It's been given to the board. We're preparing what's called an "after action" report that will probably be made public in some form in the future.

Now I'd like to just essentially give you a background of what the worm was -- what it did -- how we applied some prior successes through a DNS community and security community cooperative initiative to contain the worm for a significantly long time. Then I'll talk to you a little bit about how we felt with respect to successes and failures.

V: Yes.

V: [inaudible]

V: Yes.

Adam[?]: We're trying to [size] [inaudible]

Dave: I'm going to have to just go on while they do that, because I have to be in another meeting shortly.

Sure. Absolutely, [Tom]. No problem.

Let me start by explaining what Conflickr is. The press would tell you that it's an Internet worm. Just to explain, for those who are not familiar… A worm is a piece of malicious code that's self-replicating. That means it's able to create a copy of itself.

The nature of a worm is that it uses a network for distribution. Subsequent variance of the original Conflickr code became what's called a "blended threat." A blended threat is simply a piece of malicious code that actually uses multiple forms or methods to spread an infection.

In the case of Conflickr, the sub-variance… And a variant is -- essentially -- another generation of code. Pretty much like a piece of Microsoft software that gets updated.

Subsequent variance of Conflickr used network fileshares, maps or drives and removable media. As you can see, once it was on a PC, it could spread through an organization in a very, very fast manner.

Many people think that worms are always executable. Always little itty-bitty applications. Conflickr is actually something called a Dynamic Link Library. It's not an execution all by itself. It basically has additional code that must be somehow injected or incorporated into code that is already present on a computer.

This is the most technical slide that I have. I'll try to explain this in a non-technical manner.

What Conflickr does -- like many, many malwares -- is essentially tries to find something that's vulnerable in an operating system. In this particular case, it looks for what's called the Window Server Service. It attempts to exploit something by using a remote procedure caller -- RPC -- request, at a target computer.

The request tries to do something called a buffer overflow. A buffer overflow essentially is stuffing information into a container that's too small. The container, being too small -- and not managed -- is sort of like water flowing into a tank and then overflowing into an outer tank.

The problem is that what's in the outer tank is actually more code. Since the attacker actually knows what he wants to do, he hopes that the boundary between the inner tank and the outer tank is not monitored by the OS. Since it's not monitored, an error occurs on the OS. It allows the code to execute something called an arbitrary piece of code. That's more information or more executable that the DLL library has inserted into the Windows Service.

What does that additional code do?

The additional code actually tries to protect itself. It disables the security measures on a computer. It disables anti-virus and anti-spyware -- the Windows Firewall. A large number of updates. It actually also modifies the little DNS client on Windows Systems. So that antivirus software can't actually go up to the servers, where you download virus definitions or where you update your software for security. So it's a fairly sophisticated piece of code -- and it's remarkable to see how small it actually is.

The most important part of the Conflickr code is the code that gives what's called, "Remote Executable," or "Remote Privilege" access. This means that part of the code that's injected into Windows Server Service is actually able to communicate with other computers. Most importantly, it communicates with what are called, "Command and Control," centers. In the Conflickr terminology -- "rendezvous points." To download more malware

On your PC you now have a tiny little bit of code that is able to go up to some other place and say, "Give me some more code." This new code is what's used for some sort of attack.

In the Conflickr case, the initial code that's downloaded is what's called the "Botnet Client." A botnet client is simply a code that enlists this computer into a large army of other computers. The army itself is used for other purposes.

Just briefly, to explain what a botnet is… A botnet is an army of compromised computers that can be directed at will by the rendezvous points -- or command-and-control centers -- to do whatever malicious activity or criminal activity the operator of the botnet -- who's called the "botherder," could do. It will be part of that army for as long as the computer remains infected. Very importantly, for as long as the bots can be remotely controlled by the rendezvous points -- or by the botherder.

This is just a quick infection map of the world. I think this is as of February. Possibly May. But as you can see, there are no continents that were not affected. There were very few countries that were not affected. The overall number of infections -- which is very hard to estimate -- ranged between 6 and 17 million infected computers. It wasn't just home computers on broadband networks. It was computers in government networks. It was computers in large corporate networks.

The amount of reach that Conflickr had was incredible. What's very scary is that -- by measure of some other botnets that we've seen recently, Conflickr was small.

This is another way to look at the Conflickr infection. The clever little green-and-white cartoon map is from XKCD. It is essentially a demonstration of where all the IPV4 addresses were allocated. So, all the white blocks are the already-allocated IPV4 addresses. And all the green blocks represent grass, obviously, that can be mowed. They're the blocks that remain.

This picture is actually -- I believe -- a year and a half old. Significant amounts of that grass has already been mowed. As you know, if you've been paying attention to the IPV4 exhaustion issue.

If you look on the other map, you can see that there is a sign locus of addresses in Europe -- which is down on the lower right-hand corner. In the Asia-Pacific area, which is in the upper left-hand corner under multi-cast -- and North America. This is sort of an interesting way to illustrate -- again -- how prolific the worm was.

Many people will ask, "Well, why was remediation so hard for Conflickr? Why can't we contain this?" The same question is always asked whenever somebody talks about malware. "Why can't we simply keep it off our computers?"

One problem is that people do not patch their systems. Even when Microsoft finds a vulnerability -- as is the case of MS08-067. They found it in October of 2008. Conflickr didn't really hit the news until November. Even though it hit the news in November and the patch was available, 30% of the Windows Systems that remind vulnerable by January. The source here was Qualys -- which is a security company that does penetration testing and network monitoring and security assessment.

The other very, very big problem is that if you go back and look at some of the earlier maps and you see how significant the infection rate was in the Asia-Pacific area… One of the huge problems that we have with infections like this is pirated software. Unlicensed copies of Windows Operating Systems. These can't be patched.

Microsoft is actually trying to relax this in their code, so that in the case of a massive infection like this, even the unlicensed versions of Windows OS can be patched for security violations. I applaud them for that. I think that that's a big challenge for a company that's losing millions and millions of dollars to unlicensed operating systems. Whether you think that they can afford it or not, you can imagine if it were you.

The other thing that's very important to know is that malware writers are a very, very tenacious adversary. They're in this for the money. They are not playing games, any more.

People who herd bots -- who make these large networks -- actually lease them to other people for criminal activity. This is basically the same as taking money away from any other e-merchant.

They're going to be very, very agile. When they detect some measure to contain them, they're going to try to change it. Since they have the ability to contact rendezvous points, if they detect that somebody is removing malware in a certain manner, they will actually download that removal mechanism, analyze it and then come up with a countermeasure. Then a variant is generated and released to all the bots that have not yet been remediated.

So now you see the sort of vicious cycle that exists in trying to combat viruses and worms. The good guys go and release a patch. The bad guys analyze the patch and say, "I can get around this patch by doing this. Let me push out a new version of my little infection." The DLL. "So that I can continue to keep my army in full form and full force."

The other problem is that -- obviously, for every computer that we manage to remediate -- another one gets infected. So the botnets can sustain growth, even in the face of a fairly concerted effort to defeat them, unless we can cut off the [height of the hydra]. Which means we have to figure out a way to actually disrupt communications between the bots themselves and the command-and-control centers or rendezvous points.

I'm not going to go through any of this, other than to point out that for each variant -- for each attempt that the Conflickr writers issued to combat some measure that was attempted by the security and DNS communities to contain them… The malware writers simply raised the stakes. I'll go through a few of these in the next chronology of events that I'd like to walk through.

How do we attempt to contain Conflickr? What we had tried to do was to take some lessons from what was called the [Macao] takedown. That was an effort to contain a botnet called [Zurisby]. [Macao] was a hosting company. The hosting company had become so infested with servers [that were] operating malware sites [that were] operating drive-by download sites [that were] operating identity theft and other fraud sites. Especially pharmaceutical scam sites.

So the ISPs collectively decided, "We are simply going to disconnect them from the Internet." They literally stopped routing traffic to [Macao] and took them out of business.

The interesting thing was that the [Zurizby] bots were programmed to go to specific IP addresses that were hosted by [Macao]. So the [Zurisby] bots no longer had a command-and-control center. They couldn't be updated.

If you go and look at any of the antivirus attack trends and numbers, and you look at a graph of the period of time from September to December -- you'll notice than in November, there was a steep, steep drop to almost zero of spam and malicious sites identified.

So we were very, very effective in shutting down [Zurizby]. But of course, the malware writers were still very resilient. The people who were working with [Zurizby] decided that instead of trying to contact bots using a hard-encoded command-and-control IP address, they would generate domain names.

So they used a little random number or random letter algorithm in the code. The algorithm would generate a domain -- a string -- and then they're try to register it in dot-com. They'd register it in dot-com, and then the [Zurizby] bots would actually try to go and resolve the domain. They were smart enough to do this. Then get a new IP address and find a new command-and-control center.

When we first had the opportunity to carefully analyze [Zurizby], we reverse-engineered the payload that was injected into OSs -- and we discovered this algorithm.

Also, when we were reverse-engineering Conflickr, we found that a similar algorithm existed. We said, "Let's go and try to contain Conflickr in the same way we tried to contain [Zurisby]."

So now, I'm going to walk you through a brief chronology of events from November 2008 'til May. In November 2008, through the period of time of January 1st, the security community had identified the Conflickr A code. They'd analyzed the code and discovered the algorithm. They were preemptively registering the domains that the bots were trying to use.

So we knew when the Conflickr bots were going to attempt to do a DNS query -- to use one of the domains that they generated. The security community said, "Let's just go register them."

Well, even when you have someone cooperating, this can get to be quite expensive, if you're doing it every day for dozens of domain names. Many of these researchers were academics. They were people in not necessarily well-funded organizations, but really, really good white hats. I admire them for what they were trying to do.

The Conflickr people said, "They don't have as much money as we do. They don't have as much [nasty] as we do. We're going to raise the stakes." Instead of just using, "Com," they decided they'd start using more top-level domains, and they'd start generating more names.

So the security community sat there and said, "Well, let's see. $50,000 a day is an awful lot of money for us. We don't think we can do this. Let's go and ask the DNS community."

So they came to ICANN. They came to some of the registries, and they said, "Can you help us out, here?"

V: I'm sorry. [inaudible] [laughter]

Evan: I get enthusiastic. I'm sorry. [laughter]

The DNS community sat in a room. At the time, we had some registries that were being used. We had members of ICANN staff. We had ICANN senior management, and we said, "This is something we really ought to do."

So the registries agreed to take the list of domains [that should be] preemptively blocked. ICANN agreed that the registries would not be held in contractual violation for not paying the domain fee. The registries agreed that they wouldn't charge fees for the blocking of the domains.

And we began a process that lasted for some number of months, where we were blocking all the domains that the bots tried to register.

The first real public announcement of this effort was February 12th. Microsoft actually made a press release. In the press release, in addition to acknowledging the cooperation of the DNS community, they offered a $250,000 reward -- which is yet to be cashed in -- for the apprehension of the Conflickr writers.

To Microsoft's credit, they also put up a fair amount of money to help compensate some of the people who were paying out-of-pocket for the earlier registrations.

By February, the Conflickr writers realized that they needed to yet again raise the stakes. They attempted in the February 19th updated code to become even more aggressive in registering domains across top-level domains. They started using over 100 gTLDs and ccTLDs.

Now just having the handful of people that were meeting among the gTLD operators and the 1 or 2 ccTLDs wasn't enough. We had to really put in a significant effort to contact the ccTLD operators that were being affected, and ask them to voluntarily participate.

This was actually reasonably successful. Many of the operators were very happy to cooperate. But as you can see, sustaining this model was very, very challenging.

The Conflickr operators also decided that at this point, they really needed to try to change the way they were actually communicating between the bots and the rendezvous points. Instead of using a giant command-center-in-the-sky model, they went to a peer-to-peer model.

They injected new code in their new variants. The new code essentially said, "You no longer have to simply go to this one command-and-control center. You can go to any other peer that you can contact. We will distribute the code in this very, very flat manner across all the bots."

So the bots sort of all got a promotion, and they were all able to give their code to other bots.

There was a piece of code that was diagnosed where we realized that as sophisticated as the Conflickr writers are, they could make mistakes -- just like any other programmer. One of the things they did was, they actually put in the hard date of when they were going to do this last update. It was the April 1st date.

At first we thought it might've been a hoax. But it turned out that this was the date when one of the variants was activated. That variant essentially removed all the prior variants on the computer and installed a brand new variant that was fully peer-to-peer, and did not really rely on the domain name system for its operation.

Again, this is just one more way to look at the ccTLDs that were affected by the Conflickr infection. When we did an after-action review -- a post-mortem of what had been accomplished -- we realized some of the positive lessons. The security in the DNS communities really could work effectively at an operational level, as opposed to the policy level -- as opposed to a meeting and information-sharing level. To actually take some action and go and contain a threat.

One of the really, really interesting things about this was that the degree of trust that was extended among all the parties. These are people who never really communicate outside their own organizations very often. Introducing security and researchers from SRI and from various small operations in New Jersey to Chinese tld operators and other ccTLD operators globally was a very, very interesting experience.

Of course, Microsoft was deeply involved in this -- as was Symantec and McAffee. Microsoft is not necessarily the most well-received company in the world. So it was very, very interesting that people really worked very well together on this.

We also learned that one of the benefits the malware writers have is that they have open communications channels and they use them constantly. We manage to use communications channels to combat them.

So we actually concluded that the security and the DNS communities need each other. And we need something to carry forward, so that we can actually continue to do the kind of work that we've done to contain Conflickr, and possibly to respond to other future events.

One of the problems we have to deal with is that the collaborative response that we actually used did contain the botnets for a while. But it didn't actually put them out of business. We have to figure out other ways to deal with an adversary that is very agile and has every incentive to be as evasive or elusive as possible.

Another thing we discovered is that while it's very easy for botnets to continue their communication because they can keep spawning new ones and building little peer-to-peer networks, trying to sustain that same degree of constant communication and update was very hard among a lot of parties who have other businesses to do than to fight this botnet.

The last thing that's very challenging is that the risk-reward table still favors the adversary. They have a very low-risk, low-cost, high-reward model. We don't. We have a very high-risk, high-cost, modest-reward for good actors.

So if you think about it, the registries had to invest time, talent and expertise in taking out these names. We had lawyers scrambling everywhere. We had security people on reverse-engineering software. We have to figure out a way to change that model. Anyone who has a good idea -- see me!

Currently, we're still trying to track and contain Conflickr. We are looking at broader collaborative efforts, and improving dialogue. We are actively recruiting and working with both security and other DNS community members to establish a more resilient communications channel, and a more formal way of identifying incidents of a global nature -- and building up and operational response.

So that's it. I have time for a few questions. Thank you very much for letting me come. I apologize to the translators for speaking at [inaudible] rates.

V: Thank you, David. Any questions?

Evan? [inaudible]

Evan[?]: Nick's smiling because he probably knows where this is coming from.

V: Okay, [Evan].

Evan[?]: Have you estimated a cost of what it's cost ICANN -- the registries -- and the good parties -- to actually run after this stuff? And the second part of this question is, "How much of that has Microsoft compensated you for doing that?"

$250,000 as a bounty is garbage, when you describe what everyone has had to do. Why haven't you made the suggestion of simply -- as one alternative -- install software that doesn't get bitten by this crap?

You have one vendor that is the source of all of this grief. People who install Mac servers -- Linux servers -- Unix servers -- are oblivious to this. At least to the level they get infected. I want to know why their hasn't been a bill sent to Microsoft from ICANN and the registries that at least says there are consequences to making unsecure software.

V: Let me take off every hat I have at ICANN. Let me put on a hat that's probably going to be very unpopular here.

Microsoft certainly has problems with their OS. But it also -- as I pointed out -- is rather troublesome that a patch can come out -- the Microsoft can put the time and effort into, and identify a way to contain the threat… And two months later, still more than a third of the registered, licensed operating systems on the desktops -- even in major corporations that are also buying Microsoft software to push those patches out automatically -- are getting infected.

This is not one of those situations where you can only point the finger at Microsoft. You can point the finger at 30% of the millions of Microsoft users, as well.

V: But if the software were secure in the first place, this wouldn't have to happen.

V: But you know, that ship has sailed.

V: Can you answer me the question of, "Has a bill been sent to Microsoft for the cost of ICANN to do this?"

V: I can't. Because I don't write any checks for ICANN.

V: Do you have a budget?

V: No. I don't have a budget. I get paid to do the work that you just saw.

I'm not trying to be adversarial. I'm just saying that you're asking a question that is kind of orthogonal to what my goal is. Whether or not the code is good or bad is irrelevant to the fact that I'd want to contain the threat. I'm happy to spend time with Microsoft or anyone else, and I have in the past as a consultant -- to help them harden up the OS. But it's not a trivial effort.

I will also tell you -- having been in security for 20-some odd years… The time is coming for Linux, and the time is coming for DSD. If you pay attention to BugTraq or other listed security focuses, the numbers of threats that exist -- and the numbers of vulnerabilities that are announced on a daily basis among those OSs is staggering.

The fact of the matter is, there's just not enough interest, and the low-hanging fruit is Microsoft.

V: Forgive me -- but that's garbage. Most of the net is running Unix and Linux systems in terms of Apache.

V: Servers

V: And web servers. Right. And how many of them are spreading this stuff?

V: Actually, you'd be surprised. We can talk about this offline. They're not spreading the malware. They're hosting the compromised servers.

Honestly! I have no stock in Microsoft and I have no real reason to love them, other than that I have some friends there.

V: I'm not meaning to be really adversarial about this -- except to ask why. As an alternative to saying, "Okay -- you can do this workaround and this workaround and this workaround…" Or you can install something that won't get bit with the bug in the first place.

V: If that's the case, then there's another path. You can convince the hundreds and millions of PC users to install Linux or Mac. That's a market decision.

Other questions?

V: Mine is very brief and out of just pure curiosity. Despite the quarter-million-dollar reward, does anybody have any idea where this came from? Where the writers are from? I mean -- Bulgarian writers have certain signatures and blah-blah. Is there any idea?

V: There's speculation that it's Eastern European. But of course, there's speculation that it's Eastern European when almost anything happens, at this point. I'm not trying to be offensive to the Eastern Europeans, but that's just the way that the community is, right now.

I do apologize.

V: [inaudible] Bulgaria [inaudible]

Audience: [laughter]

V: Actually, if it's any [compensation/consolation], I was in Sofia last year and I absolutely loved it. It's a lovely, lovely city.

V: That's a lousy excuse.

Audience: [laughter]

V: While I was there, I didn't see anybody that looked like an Internet criminal.

Audience: [laughter]

V: [inaudible]

V: The communications methods you've been talking about are all IP and DNS-based.

V: Right.

V: Are you seeing movement to Skype and social networking things, where it's a completely different address space, effectively? And invisible at the IP level.

V: I personally am not. If you'd send me some e-mail, I can probably put you in touch that are analyzing Skype traffic, and looking at other platforms.

I can tell you that there are lots of…

I wrote a book on VOIP security. I can tell you that it's just an accident waiting to happen, still -- and I wrote the book in 2006.

I think that we really have to come up with some much better ways to deal with numbering spaces -- whether it's IP addresses or [e-nom] phone numbers or any private address. We're just not doing a good job.

Downloading tiny little DLLs or other applets to handhelds and phones is going to be the new wave. Especially when you look at how banks and stock companies are aggressively going after the PDA market.

I would not be surprised to see significant attacks against iPhone platforms. That's not a Microsoft product, but it's going to be a very, very sweet target. Symbian is already being attacked in many, many ways and forms.

So it could very well be the case that you'll be yelling at me why we didn't send Apple and the Symbian folks a bill two years from now.

V: [inaudible], and then [inaudible]

V: Great presentation, by the way.

The question about the country-code infections that [inaudible] Conflickr. I notice it didn't use it in the countries, if you go back to the map. Is there a reason why? Did those country codes use some sort of infrastructure or system that prevented Conflickr from using it? Or was it just an arbitrary choice by the authors?

V: I don't think anyone actually studied that yet. To be honest.

All the conversations that I've had and all the research I did to write up the after-action report, I could not find anything. So my answer is, "I don't know."

V: [inaudible]?

V: Is Conflickr IPV6 enabled?

V: Is Conflickr IPV6 enabled? I don't see that it would be very difficult to do it -- quite honestly. I think it's probably… Judging from what I looked at and from what I've seen about the code, I actually think it's probably [V6 or] V4-agnostic.

It's running as an application -- as a Windows Server service. Once it's in the peer-to-peer model, it's just actually going to try to use an interface. So my speculation -- without asking some of the really sharp reverse-engineers -- would be that, "Sure. It could run over IPV6."

V: Just a response to Dan's question. One of the things is… Much of Africa runs behind firewalls. Behind [net] firewalls. It's therefore pretty well immune to outside penetration by the original worms and things like that. I suspect that's one of the reasons that there was a lot less penetration there than other places.

The same for acting as servers. The [net] boxes effectively have protected them in many cases over the last number of years.

V: No, no -- his question related to which of the ccTLDs were used for DNS. From everything that I saw on the list, it looked very arbitrary.

V: I was really talking about the penetration by the worm, itself. Not the [inaudible]

V: Sure.

V: [Steven]? And [inaudible]

V: Looking at the kind of code that was written -- adaptability and the way it is updated. The way it was designed to get into systems…

The level of intelligence required to write the code like this -- it even surpasses the level of intelligence of people that write OSs. What makes those intelligent people to apply their minds onto something so destructive?

V: It's actually money. This is organized crime. This is not the Morris Worm kind of guy in the 1980s, who just wanted to make a bigger name than his dad. These people are electronic mafia or RBN -- the Russian Business Network.

The amount of money they are making is absolutely staggering. It's billions of dollars a year. One of the things that's really frightening about it is, they will carry the threat that they pose in the e-world into the real world. They take action against some of the responders and some of the researchers.

A lot of the researchers have to go underground once they've disclosed some of these things -- because they are physically in peril.

Law enforcement protects them. It's not a very pretty picture.

V: We are loving this, but [laughter]

V: I'm around all week, and I love talking about this. So just grab me in the hallway. Any time. Currently if you're going to buy me a beer, I'll talk to you.

V: You are not still underground?

V: I'm not underground. No.

But some of the things that we're getting involved in are scary. I've got friends who have to… not necessarily look under their car before they turn it on… But they pause and they think about it.

V: Yes. [inaudible]

Bertrand: Just before you leave, I wanted to [inaudible]

I'm Bertrand de la Chappelle -- the French GAC representative.

V: Yes.

V: This question is on a purely personal basis. I'm taking off every single hat that I wear in this environment. Just thinking back on your last comment -- talking about the electronic mafia… This is one dimension. The purpose is extortion. Fine. But it's for hire.

My question that emerged after your presentation -- regarding things like Conflickr… Is there any discussion in the security community about this being cyber-warfare testing?

V: Oh, absolutely. We've already seen examples of it last year. There's reasonable evidence that there was coordination among electronic attacks and ground attacks in Chesnia. It is definitely a real threat, and it's not just a Department of Homeland Security paranoia.

The people that do monitoring at a very, very significant level across the Internet can see this kind of activity. You can anticipate it. You can also see political use -- and misuse -- of the Internet. Even recently in the Middle East. We have to pay very careful attention.

But if you think about the way war is conducted now, one of the first things that most people do when they're going to attack a particular city or country -- they disable the communications network.

Bertrand: What I meant by that is… In the time where the big thing was biological weapons, the question was always how a germ spreads. What is the pandemic model? Does it spread in a certain way or other? Is it just by its very distribution or so?

People that are concerned about cyber warfare techniques probably need in every single region of the world to have data about how worms spread. What are the patterns of behavior? Just like when you do nuclear weapons. There are many different ways to assemble the different building blocks. To get more power, more heat or whatever.

I'm wondering -- when I see things like Conflickr or others -- how much of that is basically the equivalent of nuclear testing in the past? Like you seed one thing… the only purpose being to see how it spreads or how it doesn't. What is the rate? What is the code that can be [switched]?

Is there any discussion about this in the security community? How to prevent it?

V: Yes. There are both public and private conferences and papers. If you drop me an e-mail, I can try to find some people that might want to talk to you a little bit more about it.

V: Thank you.

V: Thank you very much.

V: Thank you.

[pause] -- [change of speaker]

V: Thanks. Hi, everybody. It's a pleasure to be here -- as usual.

The subject today that I've been asked to talk about and basically listen to questions on… Because you know -- more or less -- the situation… Is about geographic names and the new gTLD program. Particularly, geographic names at the second level.

As an introduction, some of you may have attended the GAC gNSO council discussion the other day on that subject. For me, it's an absolutely wonderful illustration of the benefits of bringing people around the same table -- instead of having them exchange letters or things like that.

We've been exchanging letters with the board -- with the gNSO -- basically for the last four months. I think we've made somehow more progress in the one hour we had face-to-face the other day than in those four months.

The current situation is the following -- if I can describe it:

There are two communities talking at two different levels. For the governments, some of them have had bad experiences with things in dot-com where there was a misuse of their geographic names of various sorts.

With the opening of a new gTLD, it's just like uncharted territory. There is a big question mark around how this will evolve. It's not only cyber-squatting -- it's also how domainers who've been very active are going to use this or not use this -- misuse it…

For those who are familiar with the domain or environment, which -- by the way -- is not composed only of bad guys… There is a very healthy financial and economic sector called Geo Domains.

So -- geographic domains -- in the domainer space -- are very, very valuable. Why? Because in many cases, you can immediately attach content -- which is travel information -- hotel reservations and flights. Just that makes them very easy to monetize.

On the other hand -- and this is more of a generic reaction, I'd say, from GAC members -- there is a sensitivity about the ownership or protection of geographic names that are very closely linked to the country.

I often say geographic names -- and especially the most famous ones -- nobody has paid more to establish a brand… I mean, there is no brand -- no commercial brand in the world -- that has been established by killing hundreds of millions of people.

So it is incredibly emotional as [Janis] was saying the other day. It's a political dimension. And it is a direct connection with sovereignty.

Basically, if you talk to a GAC member about geographic names, it is something that is very, very closely related to the nation -- the country that we represent. And very legitimately, there is a desire to make sure in this uncharted territory that maybe you overprotect a little bit at first, to avoid having to patch. To use your analogy. Instead of letting things loose and having to afterwards design processes to make sure that -- well -- you repress misuse… or you get procedures to get back the domain and so on.

The natural tendency is to say, "Wait a second. Geographic names and things of national identity of sorts are a special category of name. They must be protected in an appropriate manner."

If you look at the document that is the letter that the GAC chair sent on behalf of the GAC to the President-CEO… If you scroll down a little bit more to the bottom part… Stop.

The important thing is this… The Note 1 is a quote from the GAC gTLD Principles about two years ago, I think. It's Paragraph 27 in, "The Principles."

It says, "Applicant registrants for new gTLDs should plan to -- 1 -- adopt before the new gTLD is introduced -- appropriate procedures for blocking at no cost and upon demand of governments, public authorities or IGOs -- names with national or geographic significance at the second level of new gTLDs."

Let me stop here on the term, "Appropriate procedures." The GAC has requested in the principles that the tld applicant provide some description of the mechanism it will put in place to make sure that the governments -- without paying -- have the possibility to protect those names.

We never said -- and I think it's important to underline that this was actually a relatively open concept.

We never said, "We want a uniform procedure that applies to every single tld, to guarantee that it is protected in the same way in all TLDs."

For instance, if you dig deeper… I think it's obvious that the sensitivity of all governments regarding the use of geographic names in dot.food will be relatively different from the use of geographic names in a potential dot form -- if it ever occurs. It is obvious there will be a different sensitivity.

What is requested is that some mechanism be put into place.

Now -- let me be not the devil's advocate, but look at the other plane. The people who think or intend to apply for a new tld. The business community, in general -- of registrars and registries.

These guys are saying, "Wait a second. You are so over-protecting this thing that you're basically sterilizing a lot of very innocuous users of domain names with geographical significance that would be very beneficial for even your country," and so on.

They look at it first of all as a sterilization of some of the most valuable second-level domain property. They're afraid that actually the mechanisms to get an agreement and so on will be so complex that you'll never liberate the appropriate names. And basically, things will drag on -- and it will actually -- potentially -- in their view… and I can understand the argument…

It will actually hobble the tld of the business model. Because part of the valuable property will not be exploited. So they don't get the revenues for it. If you pay $185,000 to get the tld and so on and some of the good, valuable property is not exploited, this makes it non-valuable.

This is where we are. It's not that there is a frontal position. It's that there are two different elements that are not -- in my view -- mutually exclusive -- but that need to be reconciled, anyway. This is why the letter that we sent -- if you go a little bit higher… That's it…

The letter of the GAC is basically trying to break first step to say, "Okay. First, there is a very important element -- which is country names." Country names -- at a minimum.

There are three internationally recognized lists in the document. The ISO31661 and the two others from the UN National Group on Geographical Names and UN Member States.

Those three lists -- at a minimum -- should be reserved, period, when you launch a new gTLD at a second-level domain. But -- if you go back up a little on the first page… Yes… Stop.

What is [an interlink here] is… "It is of course the prerogative of the relevant government to adopt procedures that subsequently allow for applicants to register names from any of the lists."

Maybe it was not very clear what we're trying to do. In the exchange of letters, you'll sometimes misread what the other meant -- and so on. The explanation that I tried to put forward is, "On the one hand, there is a provision that says, 'You cut this part. It's clear-cut. And, by the way, we still need some provision that shows that for the other less-relevant domains or names of geographic significance, you have a process that allows us -- the government -- to say no'."

But governments hopefully will put into place something that would actually alleviate the burden on them. If you think about it -- and if every time a registry in a new tld is requested to register a domain name of geographic significance… if it has to ask the government, "Can I release it or not?" How do you determine that something that's being requested is of geographic significance in a country that you have never heard of?" That's 1.

2 -- if the government in question receives 300 requests a day about, "Can I get this one? Can I get this one? Can I get this one?" Nobody would be able to handle this process.

So I can imagine that -- for instance -- governments will say… That's not a GAC position, but I made the connection with the idea of categories. I could imagine that for some categories, governments would say, "Well, by the way, I have no problem with my national or country

name being used." For instance, in dot-brands… If there is a dot-Microsoft, why should a government be opposing the notion that French.Microsoft leads to the website of Microsoft dealing with French actors.

There could be a general rule saying, "Oh -- for that type of tld, we have no problem. You can use the three lists, and do sub-domains."

You could even imagine that for a certain type of travel- or tourism-related strings, the whole list of airports or the whole list of villages -- or anything in geolocalized databases can be used freely. Because it might be a very useful feature for users.

On the other hand, if the string itself is sensitive, maybe the process will require a different type of evaluation. So I just wanted to highlight this. We are not completely in agreement yet. But that's where -- basically -- the status is. I think some progress has been made in the last few days. The question is, "How are we going to catalyze an agreeable solution that provides this kind of envelope? Like activation validation and what you're allowed to do -- what you must not do -- and how you deal in the middle with what you may be doing, but need permission to do.

That's basically where it stands at the moment.

V: Let me just make a question before that.

Just going back to [dot-nation]. I was there at that time. With dot-info, we allowed companies to make their decisions about and provide…

V: Get closer to the microphone.

V: Yes… …provide some kind of reserve during some time. As far as I remember, a lot of companies -- after one or two years… I don't remember… did it.

It was really [a trick] for the dot-info to [go through it].

What I believe is now that…

Once you define very well the framework where the [accountants] should define and terminate it… That's a [dual weapon]. It's [gone/done] and that's it.

For the business side, it would be very, very difficult to wait for a long, long time for [accounts]. I remember -- Brazil, for instance… We decided to go, but the foreign affairs never moved it.

When they decided to move, it was too late. They lost. So they expanded the time.

There are lots of issues that -- from the business point of view -- certainly -- we need them to be more stable and [rectifying the] framework. I know it's difficult, but anyway, that's one point.

V: I would piggyback on this…

As always, the goal in such processes is to drive a ship between two big rocks. One rock is… The rule is very clear. But it's so bad in implementation that everybody is stuck into a regime that is hobbling everybody.

The other thing is the situation where a non-action is actually a decision. I do agree -- it's a very big problem. When you deal with governmental decisions, it is much more difficult to get a positive response than having a period of, "If you didn't answer before x-time, you're out of the game."

The problem is -- as you said -- and legitimately so… There is no way that a community like ICANN -- where all governments are not necessarily present can decide for a government that he would be bound by a deadline.

How come that I -- as the French representative in the GAC -- could at most say, "France is okay with having a system with a deadline." But how can I say that this would be imposed on countries that are not in the room?

This is one of the difficulties. We have to address this to make it workable. I think the implementable solution is the goal.

V: I have a number of different comments that are unrelated to each other. One of the things that strikes me as fundamentally problematic is, it seems that the IP constituency has gotten inside the brain of the GAC.

The very concept of treating country names as a brand -- like Coca-Cola -- I find troubling. In traditional usage, they're not treated the same way.

V: No. Of course not.

V: Right? So I see a move within ICANN to try to treat them as brands, in ways that haven't been done in current public policy.

The one thing that's bothered me most is the intent. The use of the term, "geographical significance," that goes beyond mere country names. This is where I have the biggest problem.

Just as within the gTLD community -- as they're looking to protect not "exact" names, but also "contextual" names. "Sounds-like," -- that kind of thing. I see this creeping into the approach of the GAC.

So you see protection not only for Switzerland, but also for "Swiss." Well, *Swiss* is an airline. *Canadian* is a beer. *Yankee* is a sports team. To what extent do you take something that is a representation and say, "Okay… the US government says, *Yankee* is reserved. Well, is that appropriate?

I'm just saying -- where do you draw the line? Who determines what's geographically significant? And how wide a berth do you draw around that?

I really have a concern that by taking it beyond the three names -- which I have absolutely no reservation granting should be reserved… How do you prevent that? How do you prevent this vague thing geographical significance from being totally abused?

Bertrand: The two are very valid questions. The first thing -- on the analogy of brands… I confirm that it is an analogy that shouldn't be pushed too far. I've used it to explain to a certain number of people why there is an attachment -- by making an analogy.

But you're right. All analogies must be contained. Otherwise, they bring consequences in the way you interact.

V: There's already a fear here that there's too much of an IP-protection regime going on, here. And that it seems to be affecting this, as well.

Bertrand: I fully agree that this is a danger, and it's connected to the second element that you're mentioning.

The danger -- or the difficulty that has to be addressed -- is, effectively, that in order to guarantee that things you really care about but cannot define precisely -- will not be harmed or misused. You necessarily try to cast the net that becomes then too broad.

This is a very difficult thing, because there's no way… And this is why, actually, the letter says, "As a minimum, the names of these three lists…" I think it was a nice step to say, "This is a point where there seems to be an agreement." It's relatively simple and nicely framed. Okay.

Now -- in the spirit of the non-gamable rules, which -- as you may have heard in the joint session -- I don't endorse the notion of non-gamable rules. There is no such thing as non-gamable rules.

There are things that are more or less difficult to game, and worse -- they can be rules that are gaming-inducing. It's a very important concept.

There are cases where you make the rule in a way -- intentionally or not -- where you end up with the kind of prisoner's dilemma situation. Meaning like in the security, the cost to the bad guy is very low, and the benefit is potentially high. Whereas for the good guy, it's very high-burden and very low-benefit.

The danger is to have that kind of system where either you overprotect and sterilize things, or you underprotect and you completely [game]. It's sort of systematic abuse.

By bringing the different actors together, I'm very interested in seeing how it's felt within the ALAC, because there's one actor for whom the interaction is important. To see how mechanisms can be put in place to dynamically draw the line. If I can use this expression.

The idea is that their must be a back-and-forth mechanism that helps progressively clarify relative principles. Like jurisprudence.

Imagine a government… I'm thinking about here. That's the benefit of coming to present.

Imagine that a government has once dealt with a dot-food and then dealt with another thing. Or with one type of travel-related thing. With one tld in another category, related also to tourism-and-travel. And there's a third and a fourth.

After while, hopefully, some smart guy in the government will say, "Hmm… Why don't I design a relatively homogeneous policy for things that are related to travel [types]?"

So for any travel-related site or tld, my policy is, "You can use all the names you want, but… plop, plop, plop." Period.

Then, when the new tld comes in that is in that category, they can use the document and say, "Well, I belong to that category. So I can use it."

Provided that if they abuse this, they can be slashed later on, saying, "No, no -- you're not in this category. We want it to be different." That's the way I expect it to move forward.

V: I just want to make a quick follow-up.

To use a worst-case scenario… let's say under a new gTLD -- a new dot-xxx -- or dot-porn or something like that objectionable, comes through.

Somebody wants to register French-dot-Porn.

In the print world, that isn't stoppable. It might be through the courts, if there are issues or whatever. But generally speaking, that's not stoppable. You can't stop an American group from doing something called "French Porn," as a magazine. Why should that right exist in ICANN if it doesn't exist in the rest of the world?

Bertrand: That's a very valid question. Unfortunately, it's not because we have good questions that we can have the answer.

Audience: [laughter]

Bertrand: But…

Audience: [laughter] [applause]

Bertrand: But it's a very important thing within ICANN. I've said that over and over and over again.

In many cases, we don't ask the right questions. So I think this is a very valid question. I'll tell you what…

The problem we're facing… if you look and make a comparison with trademarks, for instance… Not for the reasons you were mentioning, but because it's an analogy…

Audience: [laughter]

Bertrand: If you look at dot-com, it actually is analogous to a single global unified trademark class. If you're familiar with the trademark system, you have many classes. A typical MontBlanc is a cream and MontBlanc is a pen.

Imagine that in the trademark system, instead of having national trademark systems, plus classes that are different from each country… from the onset, you have one single global trademark class.

So the guy in Pakistan who is called Mr. Montblanc, for whatever reason, and has a shop that he wants to trademark in Pakistan… He needs to get Montblanc at the global level for any single type of activity. That's what dot-com is.

When you think of the new gTLD space, the portion of the new gTLD space will function as additional trademark classes. But the problem we're facing -- and the reason it's difficult -- is because we are trying to find a unified global regime in domains that have been incredibly nationally fragmented in the past.

What you said about French.porn is possible because of the fragmentation and the different national regimes. It's maybe allowed in…

If you take the Nazi thing… It's a very interesting discussion. For instance, you know there's a dot-gay application that's going to come in. Imagine there is a dot-Nazi guy that wants to say, "[Well, it's a cadre for the community of Nazi lovers]." Okay?

Or, "I want to do a historical type of thing that dealt with this period. Let's put this one on the slide."

Through the review process, you will have two different types of arguments. On the one hand, without prejudging of the future… I could imagine that people -- regarding the dot-gay -- would say, "It is not universally morally objectionable. The dot-Nazi might, under the general purpose, be not accepted for a gathering community."

So it's likely that one is going to be stuck at the tld-introduction level. The other one might go through. Then you get the kind of problem… Like… You're Saudi Arabia. Do you want that Saudi-Arabia.gay is allowed? Or not?

So the fact that it is unified and global brings a different level of authorization. The danger or the opportunity is on the one hand to allow openness to spread wider in many domains than it would have in the national environment. And at the same time, in certain cases, maybe extend protections in domains where it was not available before. For better or worse.

So the reason your question is a very good one is because we are changing the scale from an aggregated system based on national frameworks that try to reunify by international conventions, into a system that starts from the top and then has to accommodate the national frameworks.

It's very different. The whole new tld program -- the more I look into it -- the more I see it as an incredibly unifying factor for national jurisdiction. If I keep the analogy with what I see emerging in the trademark space… The more you get rapid-dispute mechanisms for trademarks, the more you get the full [IRP] and so on… The more you internationalize the

body of law under jurisprudence. Then you get to the national court as an implementation mechanism, afterwards.

So, the unification -- you cannot map the current system of protection and the exact frontier drawing into the global system. In certain cases, it will go further, and in some it will go weaker.

Sorry. I'm speaking too long.

V: No. We just have a [inaudible]

V: I'm partially also [inaudible] the two excellent interventions. But I still have two questions.

I've asked two questions. If you could respond, together…

The first one is about three lists. I read through the three lists and feel this is a very good list. Especially 31661. I know that is actually a ccTLD list.

Right. It's not a UN country name. So, to call it "country" may be controversial in the international environment.

V: Right. These are territory names.

V: Okay. That's perfect. Very diplomatic.

Audience: [laughter]

V: Another issue is that we do notice that something's interesting in that list. For example, there are some ccTLDs -- what we call the [Dad] ccTLDs -- such as the former Soviet Union. It's [doing] the list. Are we going to protect "Soviet Union," so that country or territorial lists…

Audience: [laughter]

V: And who is going to ask for the protection?

Audience: [laughter]

V: The Russian [inaudible]

V: No, no. That's an interesting thing. I was discussing with the Russian guy the other day…

The way dot-SU is being managed… I think the Russian government is not considering so much that it is handling dot-SU. I don't know exactly how it happens. But basically, it doesn't seem to be treated as the succession of states in international public law. When government takes over change of regime or so, there is a body of law through the ages about who gets to be the [catcher] for this issue -- for the territory -- for previous agreements and so on. I don't know exactly how they did with dot-SU. But it's a very good question.

In addition, you can even ask… I never thought of that. Very good question.

Geographic terms that are not used any more because they're related to a past regime or a past country… History. Autrichien-Hongrois -- Austrian-Hungarian Empire. Is anybody going to protect the use of "Austrian-Hungarian Empire?" It's very interesting. I don't know.

V: [inaudible]

V: Thank you, Vanda.

Is this recommendation likely to become retroactive for already-established gTLDs?

Bertrand: I don't see how it could be. Otherwise, you'd get into trouble with Amazon.com, for instance.

No. I don't think so. This is actually an interesting question -- regarding the previous question. There are people who are asking… "Hell! Didn't you ask for it before and now you're asking it in the new, regime!" In the terms of fair competition, why are the new ones hobbled in comparison with dot-com? How can you have competition with the new entrants against the one that didn't have this restriction? Blah-blah. You have to do [it] with history.

In that case, there was a very interesting argument by someone yesterday that I'd never heard. But it was in the [scaling] of the roots study session.

This person said, "You know what? If there is to be a massive expansion of TLDs, the existing TLDs in the long term would appear like a very, very small and almost non-existent part." The regime will be the regime for the new TLDs.

So the retroactive part is likely to be less important in the future. So the short answer is that no, I don't expect it to become retroactive.

V: When we talk about geographic names, is there a possibility that the future -- sometimes in 10 or 20 or 50 years down the line -- that the users from a geographical region would be grouped geographically, and the content created from a region would be confined to those geographical names?

In which case it could become possible for France to say that users from France will not access content from England, or US to say that the content created in the US is their national IP -- or a matter of their national security. So Canadians cannot access the national Internet?

I'm just throwing names -- very good names.

Bertrand: We're mostly talking here about preventing the use of the bad use of names. What you're addressing is the contrary situation -- where the geographic names are used so strongly that they become a filtering mechanism for a type of access.

V: Yes.

Bertrand: Interestingly -- if you think… Let me think a second… What comes to mind -- if I take dot-cat -- where the content in Catalan is [not] permanently in dot-cat -- but probably accessible through dot-cat… That would mean that if I am the Spanish government suddenly wanting to repress the Catalans very strongly, I suddenly decide that in Spain, no [dot-Pun-Cat] website is accessible.

It's not so much about geographic terms. I don't see that as a natural consequence immediately. But what I want to raise here is the more general question of seeing the tld space used as labels that will be used for filtering.

Let it be clear.

V: [inaudible]

Bertrand: No, no. I just want to highlight this for a very simple reason.

V: Bertrand, there was an example earlier [inaudible] the French [inaudible] case.

Bertrand: Absolutely. I was about to mention that.

V: Yahoo auctioned the Nazi memorabilia. Then the French government asked Yahoo to shut down the site.

Bertrand: Yes.

V: They said to remove it, or French citizens should not access it. They did not put a [inaudible] [inside], but this is a [difficult/typical] case, where Yahoo finally compromised. So a lot more [interesting] litigations are going to happen with many third-world parties, where there are quite a lot of…

V: I suspect we're going to have a very spirited and healthy debate and discussion at our GAC meeting. But if you'll finish your point -- there is a minuscule amount of time devoted to Evan.

I'm going to make a hard stop, because I don't need to make friends.

Bertrand: Okay. The point I wanted to make very briefly is not a GAC point. It's just a personal contribution to the discussion. Exactly in light of what we were saying…

Actually, this case is one of the reasons why I suggest that a dot-Nazi would be a globally unacceptable norm, worldwide. Yes.

The point that we are facing when we say, "Filtering," is… Let's be honest. All countries not only do, but must, filter according to the national law. The [other] case was that there is a law in France that makes it illegal to sell those wares. So it's an application of [this law and that].

Which means that in certain cases, you may have governments -- because of their sensitivity to a specific tld -- that will say, "We don't want -- in our country -- access to that tld to be for our citizens." But -- there's a strong difference between having a national legislative process

that clearly defines the rules and why something is being forbidden because it is illegal, and the ad hoc filtering of words of a certain geographic significance.

Audience: [laughter]

Bertrand: I don't want to get into this debate. But we have to be aware that in the evolution of the gTLD space, when we will accept strings, the contentious strings will have to be divided between the ones that are sufficiently morally unacceptable globally to not be allowed at all -- those who are so morally acceptable by everybody -- or politically acceptable -- that nobody [would be upset].

V: And the [inaudible]

Bertrand: And the ones in the middle that would be not enough to be refused by everybody, but sufficiently objectionable by certain national governments, that would say, "By legal process…"

V: We don't all want to be vanilla, so that's a very, very good thing. Evan? And then a final word.

Evan: I've got a very short question that could take a long answer. But I'll frame it in a way that takes a short answer.

Audience: [laughter] [inaudible]

Evan: Has there been discussion within the GAC of whether or not this is appropriate for ICANN? Or perhaps a broader treaty system? Because what you're talking about with its level of diplomacy sometimes almost sounds like a treaty organization more than a technical body.

Bertrand: The last point I was making? Or the geographical names?

V: The geographical names. Just [inaudible]

Bertrand: Interesting question. I think the short answer is, "Not really." It is being discussed within the confines of ICANN. Actually, what you're saying shows that ICANN can be -- when it works well -- a nice space for dealing with very sensitive political issues. If it is done well. I hope it will be.

V: But certainly our intention…

V: [inaudible] aggressive [inaudible]

V: Bertrand, it's always a pleasure to have you in our room. You always leave the audience wanting more. But I know we'll be meeting in the back room.

So in the very politest way, may I ask you all to thank Bertrand for his time and effort.

Audience: [applause]

Bertrand: One last word, if I may.

V: As if I would stop you.

Bertrand: Just one last word. There is a very interesting and important issue that we need to all address together. If you were in the SOAC discussion yesterday, there was a theme about prioritization. Making prioritization the subject.

The outcome I get and that I hoped was going to come out of the SOAC discussion is that there is a priority issue now emerging. That is the institutional evolution of ICANN.

In a nutshell, we will have between September 30th and June of next year, a window of time that must produce appropriately reformed bylaws.

To what extent this is a broader charter or just a reform of the bylaws is up for discussion. But I think that interaction and a joint message by the different actors…

V: You're talking to the most cooperative lot we can drag together. So I'm sure we'll be into that [inaudible].

Thank you, Bertrand.

If I can welcome Maria to the table, now… We're moving to the *Improving Institutional Confidence* section of our agenda.

We have a hard stop at 11. In fact, a moment before 11. So I'll let you stand up. You're more than welcome.

V: [inaudible]

V: Yes. You'll be on the queue, though.

One thing I would just like to remind those who are listening on the audio bridge… We will now be moving to a "next," or "new" room. So -- no we're not?

V: Same room.

V: Same room for this discussion? That's fine. Okay. We can stay in the same room. Whew! That's all right.

That was a misunderstanding between me and the powers-that-be to the left. I thought we were moving to a new room.

Maria -- thank you so much for your time and energy here today. And the fact that you don't have slides is a godsend. You can tell we're rather an interactive lot, and we don't necessarily need to look at pretty pictures. The floor is yours.

Maria: Thanks very much, Carolyn. Thanks, everyone, for having me here today.

Actually, just a quick question… How much time do we have?

V: 20.

Maria: 20 minutes. Okay. I'll try to keep my talking as short as I can, and do a quick q-and-a.

First things, first. Improving institutional confidence. The first thing to be said is, "Thank you very much," to the At-Large Advisory Committee for providing details and very thoughtful comments. Kieren McCarthy was able to ensure that they were part of the public records and also part of the summary and analysis of comments. That, and also the ideas in them were made sure to be part of the deliberations of the board. So thank you very much for providing those.

Secondly, Item 2. The process. I'm just going to talk you very briefly through what the process is going forward, on improving institutional confidence.

The President's Strategy Committee was a committee set up by Paul Twomey to look at strategic issues facing ICANN, and to try to basically put the minds of the good and the great together -- to keep… Apologies. Yes. Sorry. That's my Irish. I'm quick-speaking.

V: The Spanish are doing their best to keep up with you.

Maria: Right. Yes. I need to say less more slowly. Okay.

The PSC -- President's Strategy Committee -- has carried a lot of the load on the thoughts of the strategic issues facing ICANN, going forward. They've done a lot of work over the last year to have consultations with community and to be basically a brain truss or a think tank on these issues.

Particularly to do with accountability, internationalization and some other issues -- including security and financial… Both operational security and financial security and security and stability of the Internet as it relates to the [IRT] and other issues.

They did their work. They presented a final report to the board, which was in Mexico City. Process-wise, where we are is, the board is looking at that report and thinking about it.

Whilst it's been thinking about it, it also asked the staff to look at producing a document with suggestions on how all of these great ideas the PSC had could actually be implemented.

So the staff has done that. On the 1st of June, they produce a report. We published it on the website. It's not yet translated -- for my apologies. However, this document looks what the between 20 and 30 recommendations of the PSC -- how they can be parsed out or organized in such a way that we can focus on the really key issues of concern to the community.

So that document was published. The board is thinking about it. There will be discussions at the board meeting on Friday as to where to go with that. Part of the recommendations of the staff were that we should look at bylaw changes on two key issues. Basically, on accountability.

One on a mechanism for the community -- by a 2/3 vote of the SOs and access -- to be able to require or force the board to reconsider a decision. And secondly, to create a new,

independent review tribunal -- which unfortunately has the acronym of IRT. We may try to work on that one.

To look at a new IRT -- IRT-Mark 2… As a group of independent, judicial and potentially technical experts. But mostly, focusing on traditional experts to review decisions by the board.

So this was as a response to the community's very strong and very clear message that it was not enough for the board just simply to reconsider or review its own decisions. There needed to be an external mechanism -- external to the board and to ICANN, itself.

Those are two bylaw changes that the staff has proposed, which the board has certainly not yet made a decision on. But we have posted that they should consider making those bylaw changes.

Potentially, this was the staff recommendation. We have proposed the board go ahead with bylaw changes on those, and propose them beginning at its meeting on Friday, and then begin the process required for bylaw changes -- which would be public consultations, further deliberations by the board and the community -- in a process that would take approximately 3 months.

If the board had mature-enough discussions on the issues this week -- and if they do decide to go ahead with bylaw change, they will defer their public consultations really on the nitty-gritty, specific details of what that bylaw change might be.

So that is a big "if." I'm just trying to lay out for you where this process may go. The board may well decide it needs more time.

The other aspect of the process really is, "What do we do this week to be part of this discussion?"

First off, there is going to be further consultative meetings tomorrow -- Wednesday -- 1.00 to 2.30 pm, here in Sydney. So you're all very much invited and encouraged to attend. I feel quite confident that there will be questions on this coming up in the public forum on Thursday. So those will be the main moments for input during this week.

I am putting together a two-page cheat sheet or summary of these proposals. Where they come from, what the really key proposals are, and where they're going. I see that very kindly the At-Large staff has zeroed in on the display here on the board -- of the really key issues -- which I'm going to give a very short [presentation] of, if I may.

We have adopted the principle… Well… I'd like to think we've adopted the principle of subsidiarity as a good European girl. The principle of subsidiarity, basically, is a complicated EU concept. It's to explain something simple -- where you've got a lot of decision to make. Let's push the decision down ideally to the most suitable body to make that decision.

In this instance here, we've suggested to staff that we take a lot of the issues that perhaps could be dealt with by in-operational planning and in our financial and budgeting planning. For example, at the gNSO review and implementation.

Actually, don't scroll for a moment. I'm going to come back to this. I promise you.

We've basically taken all of the other issues, which we believe are not crucial to this particular discussion here. We've taken all of the issues that can be dealt with -- we believe -- more effectively in another part of the organization, and put them there.

Sébastien Bachollet, I believe, has created a document that's based on the table that we've put together, saying, "Here are the 20-plus recommendations." He's actually created another column for you guys to put your input in. That's brilliant!

So we basically said, "This issue should go to the gNSO Review. That issue should go elsewhere." The three top issues, which we have decided to keep… Well, which we recommended that the board keep in the absolute center of its vision here are… The accountability, which I just discussed…

V: [inaudible] on the screen. [inaudible] [laughter]

Maria: I was afraid I was making you dizzy, there, for a moment.

So we basically focused on saying to the board, "Listen, guys. You need to focus on three issues, here. 1 -- internationalization. 2 -- the GAC and 3 -- board accountability mechanisms.

So, I'm just going to tell you a little bit about the substance of these issues, and if I may, just refer while I'm doing so to some of the points that were raised in the comments by the At-Large Advisory Committee to the public comments, which finished in May. Just to try to address some of your points, and let you know how they've been responded to or dealt with.

First off, board accountability mechanisms. We have a very strong view from At-Large and the committee, in general. As I mentioned before, it's not sufficient to have just internal accountability for the board. External accountability is key. So that is being moved on.

Let me just go back. Actually, that was the main point on accountability mechanisms.

On internationalization, the At-Large Advisory Committee had some very sensible points. Those were that the real internationalization that ICANN is doing is in its operations and its day-to-day ability to allow people around the world to interact and participate.

So we have said, "Yes." Translation and interpretation are key. This is how they should be dealt with operationally."

Staff recommendation on what the PSC considered to be the central issue with internationalization… That was whether ICANN should have different legal presences in different parts of the world. I think we can say probably quite fairly that response from the community was lukewarm, at best on this proposal.

The community and the At-Large also did not find the there was enough of a rationale for doing so right now -- based on the information that we have.

So the staff proposed to the board that we should continue to finding out more about what the benefits and the potential drawbacks are of having ICANN legal presences in more jurisdictions outside of the US. We've also proposed that -- yes -- we should continue to maintain our legal and operational headquarters in the United States.

If and when we find more information about internationalization in terms of legal presence, we should come back to the community and make a decision on it.

I say this objectively, but I do think it's fair to say that this issue is not the most important of the three top issues that we recognized. I think we have to recognize that the community does not find this to be a Number-1 priority at this time.

The priorities, going forward, I think are going to be these two accountability mechanisms -- and also, just moving forward, onto the role of the governmental advisory committee.

Regarding the role of the GAC… I guess what's probably fair enough to say is that we've simply recommended that the board make a decision to move forward in a fairly active way with what is one of our responsibilities under the JPA affirmation of responsibilities. I'm going to read it off the screen.

ICANN should work with the GAC members to review the GAC's role within ICANN, in order to facilitate effective consideration of GAC's advice on public policy.

We broaden that to say also that it needs to be -- Number 1 -- a community-wide discussion, and not simply a discussion between the GAC and the board of directors. It needs to be a consultative discussion, and it also needs to be a broader discussion about how the GAC can operate more effectively within the ICANN system.

I don't think they're speaking out of turn there, because indeed the GAC itself has said that it wants to operate more effectively and be integrated more fully into the ICANN system.

Coming back to some of the comments that we received from the At-Large Advisory Committee on this particular issue… One of the suggestions received was that the ALAC should potentially be on a similar -- what I'll call a -- "status". Because it's not a bylaw issue. But on a similar status to the GAC.

In that when the ALAC or the At-Large structures make suggestions or recommendations or requests for policy issues to be considered, the board should respond to them in the same way it's begun responding to the GAC. So that was one of the issues that was raised by the At-Large Advisory Committee. I don't have anything particular to say on that, except to observe that we don't have a bylaw requirement for the GAC to get a response. As far as I know… I don't think I'm wrong, there.

V: Yes. [inaudible] [crossing]

Maria: Oh -- I apologize. But yes, we don't have a bylaw requirement for the board to make a response every time the GAC communicates. We're trying to get a better process to do that.

There isn't one currently to require that for the At-Large. So I think that's new and novel idea to the process. It's certainly something we should push, going forward. I'll be quite honest and say it's not something that the staff had put into the recommendations.

I think that's something that you guys probably could and should push. But we've not considered it in the recommendations that we've made. We've considered it, but we've not included it.

So just to conclude here, I suppose… On capture is the final issue that had been discussed in a big way in the At-Large ALAC comments. I think the fundamental insight there really is that capture is best avoided not simply by rules and 2/3 or 2/3, but more through increasing and facilitating proper participation through the organization. Be it via languages and interpretation -- be it via better remote participation.

I think that's a fundamental insight that is certainly very much part of the staff recommendations. Though what we've suggested be done with that, basically, is to push the interpretation of those issues to where they belong.

For example -- to the Public Participation Committee -- to Operational Planning and those sorts of things. I can recognize fully that it may not be the most satisfying response, because it would be nice to have all of these things. And other issues in the PSC or in the board focus in this respect, with this *Improving Institutional Confidence* issue…

However, I do think that we can work most effectively as an organization if we manage these issues where we think they can be best managed -- but in a detailed way -- by the people responsible for them. That is clearly going to be a subject for discussion.

I must say that I personally, particularly, would welcome peoples' input on that. I would also -- if I may -- before we kick off into q-and-a -- ask if we have got it right. If from your reading of all of these 20-plus issues, have we identified the top 3 issues? Should we be recommending? Should we have recommended that the board begin bylaw changes? And if not, what are the issues and how should they best be adopted or addressed? How would you like to see this thing, going forward?

Thank you all very much for your time. Looking forward to questions.

V: Thank you, indeed. I did recognize Evan earlier on, so please go ahead, Evan.

Evan: I'll save it to the last, because I've been sort of monopolizing things 'til now.

V: Trust me -- you won't monopolize. I don't see anyone else's light on or hand waving. So feel free.

Evan: In response to what you said was probably the least-important thing on your list… there was a very engaging discussion going on in some of the chatrooms earlier about alternate incorporation locations and rationale.

Especially in a potentially post-JPA world… Ultimately… There might be an idea -- at the very least -- for optics of ICANN being seen as not just an American organization.

There might be some appeal to the idea of if there are legal prohibitions from leaving the US to having a secondary presence.

So while it was at the bottom of your list, I think there is still some keen interest in that, in some circles.

Maria: I guess my response to that is, "Fair enough." That's interesting. It's a good thing to hear. I will say quite bluntly that this proposal has been seen very strongly as something that the staff was pushing. And for which there was not huge response or warmth in the community.

When I look back at the three public comment periods we've had over the last year, we've been getting told again and again… And at every meeting we've held on this… "Listen, guys. This is not a priority for us. Sort out you accountability."

V: [inaudible]

Maria: Yes. So I do recognize you're talking about degrees of priority. If that's becoming an issue on the radar, then -- yes.

V: Perhaps over the horizon radar. But that will come at some point.

I recognize Alan, then Adam, then [Hon].

Adam: Yes. I wanted to ask something about accountability mechanisms in this new 2/3 thingy. 2/3 vote or requirement by the SOs and ACs to reconsider an opinion. Could you go through it?

When it was described to me, it sounded like there was an unnecessary middle step in there. I can't remember enough details to remember what the unnecessary middle step was. So perhaps if you could run through what they are, then I might actually get my memory back.

Maria: Sure. I'll do my best, Adam, to describe. I'd have to say a proposal which isn't completely fleshed out. I'm going to read from my own CribNotes, here. What we say in this staff recommendation follows on from work that's been through the PSC for quite a while, now…

There should be a special mechanism for the community to require the board to reexamine a board decision -- invoked by a 2/3 majority vote of 2/3 of all the councils of all the supporting organizations. And, 2/3 of members of all the advisory committees, and strong support from the community.

Now -- I'm going to speak slightly perhaps out of turn and say, "This is a proposal that sounds like it's very detailed." But actually, once you think about it, there's an awful lot of figuring out how that would work, in practice.

One of the key issues is going to be fleshing out how that works. I think the idea here was to have some sort of intermediary step between the nuclear option -- which was in previous proposals. That had been having a 2/3 of a 2/3 vote -- which could potentially be called

"Spilling the Board." For the interpreters, I don't think that's quite an adequate expression. Basically requiring the board to step down in some form.

There's been a whole complicated and lengthy legal discussion of whether the board could be required to do so, as it's a non-profit organization in California, and that that's not possible. They could have their resignations pre-offered. That seemed like a good idea, but then other legal opinions said it was impossible.

I guess the short answer to that question is, "This is the middle option between saying to the board, 'We disagree with you, but there's nothing we can do about it,' and firing the board."

So this potential bylaw change is still in the cards.

Adam: I think the issue would've been that it was the word "re-examine." If you have such a strong documented opinion of the community, it's not a matter of reexamining. It's the fact that, "You will do this." It's not, "We're not asking you to look again," because there've been board reconsideration committees that have been completely ineffectual. It's the wording of "reexamine," that I think is the unnecessary step.

It's the community saying, "Board -- no -- you've got it wrong. Start again." There's a stronger element than the word, "reexamine," that's perhaps what I'm trying to get at. But I'm losing something with a previous… There's something that I'm forgetting in terms of this. I'm not being very helpful.

Maria: Just to say I think my own explanation is somewhat inadequate. Probably John Jeffrey could do a better job of explaining it to you. I will remark, though, that I think what you've suggested -- where the community through this 2/3 of 2/3 mechanism would require the board to not just reconsider or reexamine or review or basically, "just do over," what it's done…

Probably, I'd imagine it's been proposed. Because the chances of the community ever agreeing to a very fine-grained degree… "Broad, you didn't just get it wrong. You got it wrong, and now we want you to decide that way…" I think it's a fairly rare-enough proposition. But that's purely personal commentary on it.

V: An intervention by Nick. And then it is Alan and then [Hon].

Nick: I suspect that is meant by, "reconsideration," is "reconsideration as contained in rules-and-procedures for meetings." Where reconsideration of a decision is triggered by a decision of the body that made the original decision.

This is suggesting, I believe, that this is automatic. The board's reconsideration of its own decision is automatically triggered by a 2/3 vote of the community. Traditionally, a 2/3 vote is what is required under rules-and-procedures of meetings, to reconsider an issue.

So I suspect it could simply be explained better what exactly is meant by that.

Maria: Thanks a million for that. That's a good point.

Adam: [inaudible]

V: [inaudible]

I'll clarify it. Go ahead. Thank you, Alan.

Alan: Two points. One of them goes back to what Bertrand was saying when he was here -- talking about the reaction of countries to any given top-level domain. It has a wide range, from "Who cares?" to, "Under no conditions will anyone accept this."

The concept of responses from the board to an advisory committee have a similar range. They range from, "They must obey everything we say in our advice," to the other end, where, "It would be nice to have an acknowledgement that the e-mail was received."

Right now, we are beyond that last tail. Not only do we not see the action -- not only do we not get a reason why -- we're not even sure it was received, sometimes.

That may be what is triggering some of the strong statements you hear. We don't know if the e-mail failed. Or if they didn't care. Or whatever.

So it's that range of things that I think one has to consider when looking at the statements and suggestions. We could be satisfied really easy in some cases.

V: You're not too tough a nut to work with. But when the simplicity of an auto-responded "read" receipt is not even part of the protocol, I think that's pretty piss-poor performance. And I do hope that is translated accurately.

Audience: [laughter]

Alan: And of course, once we get the confirmation, it would be really nice to know that the mail went out to the board in a timely manner. Not 14 days later.

Sorry. Okay. That was the simple one.

Audience: [laughter]

Alan: We talked a little bit about the issue of "Capture," yesterday at the ACSO meeting. There was a discussion of the issue of "Trust and Transparency." They're all closely linked.

If you can see how a process unfolded, the issue of "Capture," is not nearly as strong. Because it's visible, and if you don't like it, you can object. It's not just a black box.

To those who follow politics in the UK -- which I don't… But I'm not completely oblivious… There is a current scandal going on. A government that ran an election on a platform of transparency is proving to be a little bit less than completely transparent.

As I was flying through an airport lounge on the way here, I took out this front page.

V: Just for the audio -- it says…

Alan: Transparency -- what a joke! And it shows a burning tank.

Maria: I will say, I wouldn't believe a thing I read in the *Daily Mail*.

Alan: I don't have to believe it. It just seemed to apply so much to the meeting I was going to, that I took it with me.

V: Wouldn't it be nice if that wasn't the case for us to be so motivated?

Maria: If I may just say… I gave a fairly short shrift -- or I didn't give a sufficient explanation of this independent review tribunal.

There are two things that are special about it. One is that it exists autonomously and apart from the ICANN and its board. That's a very good thing that it would exist in the way that we imagined it as staff.

The second thing that's important about it is that it gets to review a decision -- based on two things. 1 -- how a decision was made by the board. So if the right processes were gone through, et cetera, it would go somewhat to this reconsideration issue. Which -- I think -- the community has found to be insufficient.

The second thing is that it gets to review a decision, based to some extent on the substance of that decision. On what was decided, and were the correct issues looked at. Were they looked at in the right way? Was the balance of any imposition on peoples' rights… Was the balance weighed up correctly?

So there is a fair bit of detail of the rubrics or the principles under which the substance of a board decision can be reexamined by an external body. I think that's probably a fairly key and quite important development -- which does slightly address those concerns.

V: You must feel you're in the hot seat. I do want to move to [Hon] as quickly as possible.

Alan: Yes. Just a quick follow-on. It's important to have that process clear and effective. They way you've described, it's very positive.

It is more important to have the ongoing set of processes such that you don't need that process very often -- or ever.

V: I doubt that there's any response required to that other than absolute agreement.

Thank you. Hon -- go ahead.

Hon: I will be as quick as possible.

My question is also related to IRT. Thank you very much to Alan for raising this. Maria has already answered part of my question.

But I still have a question on IRT. I noticed very early [what really would turn up].

My question is, "Will the IRT be institutionalized? Or will it be on an ad hoc basis?" This is quite important. It means that a group of people -- most probably retired judges -- going to try

all kinds of cases… or that it will be ad hoc. [Which is international criminal code for former Yugoslavia]. [Or criminal code] for Cambodia or Khmer Rouge. They're case-by-case. I guess this is quite important.

In the JPA public consultation, myself and a couple other international scholars submitted our proposals on this tribunal already. We suggest it should be a [inaudible] distributive ad hoc [inaudible]

V: A rousing, "Here-here!" Go ahead, Maria.

Maria: Interesting. The way it's been conceived is as a standing body of people with a 5-year term.

V: We're about to start petitioning. Can we get the working groups in order? I want the ALSs ready to rock-and-roll on that one.

Maria: I will say I'm actually surprised. I'm personally surprised. I would've thought -- as a former political student -- but clearly, I've got this wrong and I'm missing something… But I would've thought you'd think it was a good thing that there would be a standing board or a standing group of people that could build up some authority and expertise, and who would not be basically in question of shuffling the chairs around every time we have to make a new decision.

It does look like -- to me -- that we're looking at [Hon]'s [constitutions]. And John Jeffrey is clearly the expert. But myself, in looking at it, it seems to me that there would be a large-ish pile of people with a variety of expertise, on whom we could poll for specific issues. But that these would be people that had agreed in advance. And I should hope, they'd familiarized themselves with ICANN and its processes.

V: Maria -- take a deep breath. The way you presented it then was vastly different to our initial reading. Especially when we're not working with English as our first language. You've got a puddle of appropriately -- and I do mean "puddle…" "Pond," would be better, but let's work with "puddle," to begin with… of an appropriately skilled set of individuals from whence that selection process happens. That is much closer to exactly what [Hon] was mentioning in the papers. That's not the first read.

We can get very hysterical very quickly. But we're easy to calm down.

Maria: Well, I hope I haven't calmed you down on the basis of my interpretation -- perhaps not the best. But I'll read out to you what it says. I think I'm going to make a point to ask for tomorrow's meeting, to try to go through this and give a bit more detail.

V: Yes.

Maria: That's clearly going to be an important issue.

What we have proposed [to staff] in the document is the independent review tribunal should consist of a standing panel of internationally recognized, relevant technical experts -- as well as internationally recognized tourists. Including persons with senior appellate judge experience.

Members should be appointed for either a set period of five years, or until they resign. That's basically all it says about the membership. So, we'll hear some more about that tomorrow. I'll make a note and ask for us to provide more detail of what we might have imagined.

I think the really important thing about tomorrow is to look at this document as, "Well, yes -- it's a nice idea. But what we really need is to hear from you."

I suspect we're getting close to closing comments. Mine would be simply that we do… This is purely a staff proposal. It is something that the board needs to consider. I think of that very deeply.

We really need to hear, "Does this work?" And, "What should such a [panel] list look like," for example. We really do need people to weigh in and give your considered thoughts on what's going to work and what's not.

I'd imagine… I'm not speaking for the board, but I'd imagine… One of the board members just [left]. Oh -- there you are! [Roberto]. Sorry.

V: Are board members appearing?

Maria: Appearing and disappearing. I'd imagine it would be very helpful for the board in its deliberations to get a very good view of what the community's initial reactions are to this, and what they think will work and won't. So please do come along.

A final plug for this cheat sheet -- which I will be preparing in the next hour -- which will be on the ICANN booth table beside the registration desk… We will also -- by tomorrow morning -- have it translated into Spanish and French -- to help people have at least some kind of summary overview of this.

V: Thank you very much, Maria. I must say, it's another one of those exercises where you've left us wanting more. That's always a good thing.

We've had to spread ourselves thinly. We will have members of our community that have a mandated requirement to post their reports on the meetings they attend to the general community -- in your grouping, and in many others. We'll be briefing them. So frantic Skyping and chats go on around all of this. We, too, multitask -- not just the board.

We would like to thank you in the usual way for what I think was a very, very worthwhile explanation and exploration of improving institutional confidence. Thank you.

Audience: [applause]

V: In terms of housekeeping, now -- how many members are we expecting? [Roberta] -- welcome. 2 or 3?

V: We are expecting 4.

V: 4.

V: So it's myself, Harold, [Beimundo] and Wendy.

V: Ah -- Wendy.

Well, Wendy knows all too well that we're not going to let her stay in the background. If you are a regional representative or a liaison, and you can vacate your seat for two more board members, that would be… shall we say… if not appreciated, mandatory in just a moment's time.

Audience: [laughter]

V: So we are missing just one member?

V: Okay. Let's stand up, while you're unplugging your power cords -- for those of you who decided it would be a discretionary thing to do to back off and let our guests sit down.

Stand up -- stretch -- and when [Romundo] arrives, he'll have a place and a space at the table.

Wendy's going to come and kick somebody out. [laughter] Thank you. Thank you. [laughter]

Just to now remind everybody -- this is not a streamed meeting. This is a meeting which is not being streamed. It's not being audio-cast and it's not being recorded in an Adobe Chatroom in any way, shape or form. This is an informal exploration between the Structural Improvements Committee and the At-Large Advisory Committee and the regional leads we have here today.

I'm doing my best to work it out. Is it to stream or not to stream?

V: No.

V: It wasn't meant to be. And it is not streaming. Okay. Thank you.

So, Wendy's got a home. Plugging in power. [laughter] It's just moving. Yes.

[Romundo] can take over where [Shiva] was sitting. That looks very well. We've got everyone.

Who is the lead? Who's going to do the introduction? Is this you, [Roberto]? You're going to run it?

Okay. In that case, while Wendy's plugging in and getting settled down, I'm going to hand it over to… I'd like to think we still have a proprietal interest, seeing as you came from ALAC [laughter] to the lofty heights of Deputy Chair.

If I could hand it to you, we'll have a little interchange and then a discussion. I'm assuming an interactive, open conversation.

[session ends]