MARRAKECH – Fellowship Afternoon Sessions
Wednesday, March 09, 2016 – 18:00 to 19:30 WET
ICANN55 | Marrakech, Morocco

UNIDENTIFIED MALE: Fellowship afternoon sessions, [tech Alex] [inaudible].

UNIDENTIFIED FEMALE: Good afternoon, everyone. Wow. That's a doozy. Check that out. Everyone awake? Anyone who is sleeping is not now. So we have a little bit of a strange afternoon because the gala buses start leaving at 7:00 P.M. So we want to try and make the most of our speakers' time.The last meeting before us went a little bit late, and as loud as we were trying to be outside, they just weren't getting the picture. What are we going to do? In any case, we went a little bit over this morning, so that was our punishment.

Thank you all for being here. All of you have had a good day, I hope. Tomorrow morning, we're going to get a longer opportunity to go in and talk about the week that we've had. Usually, we try to use these afternoon sessions to do that, but we've had so many speakers come in in the afternoon, we haven't had that opportunity so I wanted to let you know we're going to have that opportunity tomorrow.

For our speakers this afternoon, Steve Conte and John Crain are ICANN staff. They're two of my colleagues and they're here to talk to us. What are you here to talk to us about, gents?

STEVE CONTE: I don't know yet.

UNIDENTIFIED FEMALE: Okay. I told you that you had to prepare at least ten minutes beforehand, so go ahead.

STEVE CONTE: How much time do we have because I know you can do a download] too, right?

UNIDENTIFIED FEMALE: Yeah, I want to try and let them go by about probably five or ten minutes to 7:00 so that they have time. There are other shuttles, by the way. It's not the only shuttle. It's just the first shuttle leaves at 7:00, so I want to get you out of here before 7:00. It is close to 20 after 6:00, so we want to give ample time for questions.

JOHN CRAIN: Okay, well, I'd normally say that we're between you and beer, but I heard the gala is dry, so we're between you and water which is still good because I'm sure the food will be great. How many of you are first time fellows? How many of you have seen me speak before? All right, so I'm not going to do the slide sets.

I'm the Chief SSR Officer, Security, Stability and Resiliency at ICANN. I run a small group, of which Steve is one. We look at the security of the identifier systems, domain name system, routing, etc.

We're short on time, so I'm going to go straight to questions. Who has questions about Internet or identifier security, stability or resiliency, or maybe some of the things we do like training programs? We're the group that do a lot of training programs, and we're also part of the group that does a lot of research. We can sit here and do slide sets, but does anybody have questions for us? I'm going to start with the young lady over here. Do you want to use this microphone?

UNIDENTIFIED FEMALE: [inaudible] [Tajani]. Can you start by telling us what aspects of security you are looking at in IPv4 and IPv6, maybe? Like identifier, like resources?

JOHN CRAIN: So IPv6, we're actually not doing a lot at the moment. Some of the issues we had in the past were making sure that IPv6 was deployable. So when we look at the ICANN side, it's things like if I want to use IPv6 in the DNS, for example, because DNS is about translating names, can you actually do that? If I'm an end user, can I actually put my quad-As, my IP addresses into the DNS? If you look around at the registrars, mostly you can now.

So these are two of the things we were looking at. We were looking at things like if we put quad-As into the root zone – this was a few years ago and, of course, we've done this – what's the effect? What will we break by changing the size of the root zone, which is a DNS file for the TLDs for the Internet? What would we break? We look at things like that. We look at things and say, "Well, how is this going to change things?"

If you look at IP Version 4, v6 has one commonality with this. There are two interesting problems at the moment. One of them is the fact that you cannot authenticate who owns which IP block. Who here plays with routers? I'm very jealous. They took all of my enable passwords away years ago. I'm not allowed around routers anymore.

You can secure between two purists, two people talking. You can use MD5 or some other algorithm to authenticate who you are. You can't do that globally. There have been multiple attempts to

fix that. Secure BGP is one of them. BGP is the routing protocol, a secure version, and something called RPKI, Routing Public Key Infrastructure. Neither of those have really been that far deployed. So those are the kind of security issues we looked [at] there.

The other one is there is something, they call it gray market, the emerging market, the IP Version 4 market.

You might not think that's a security issue. Why is the fact that people are buying and selling IP addresses a security issue? It's not, but it might be a stability issue. What if, five years from now or two years from now, addresses become so expensive and so limited that none of you can get them? In a way, that means you can't even do the translation that we do between v4 and v6. I'm not saying that's going to happen, but that's something we got to look at, and people are starting to study this.

I'd say about five or six years ago, we had a workshop that Google hosted that looked at whether or not there would be an emerging market. We predicted that there would be, and we were looking to see if we could put controls in it. With some of the best economists in the world and some great engineering people, we couldn't figure it out. So those are the kinds of things we look in the address space.

Obviously, the resource depletion of IPv4 is something we've been looking at for years and trying to get people to understand that it really was going to happen. Unfortunately, people never believe you when you tell them the sky is falling until it lands on their head.

We've been saying, "IPv4 is running out. IPv4 is going to run out. No, seriously, it's going to run out really soon, soon."

Everybody says, "Yeah, yeah, whatever," and then one day, IANA, the ICANN block, ran out.

We try and predict these things, even though people won't listen. We're really looking at that side of it more than getting down into the nitty-gritty security details.

UNIDENTIFIED FEMALE: [inaudible]

JOHN CRAIN: Yeah.

UNIDENTIFIED FEMALE: First of all, I think that the RIRs are also looking into the issues of RPKI and IPv6.

JOHN CRAIN: Absolutely.

UNIDENTIFIED FEMALE: So where is the border between what ICANN is doing and what RIRs are doing? Secondly, at the beginning, I thought that your group is working at infrastructure level, but now it seems to be end to end operations. Is that correct?

JOHN CRAIN: We're looking at protocols as well. We're looking at the things that use the identifiers. The central thing is the identifier system. Those are names and addresses, port numbers, all of the identifier systems. And yes, the RIRs are, of course, looking at all of the things around IP addresses and also, of course, autonomous system numbers. So we work together.

I used to work at the RIPE NCC. They have something there called RIPE labs, which is a research center within one of the RIRs, and we work very closely with them. In fact, who's heard of the ATLAS program? We're one of the sponsors of that program. Daniel Karrenberg, the guy who designed it, is one of my best friends, so we work on this kind of stuff together.

So is there a border? Definitely when you get into the policy realm, but when you get into actually working on real problems, we tend to work together a lot.

OSAMA TAMIMI: Good evening. I'm an ICANN fellow from Pakistan. I just have a general concern. Are you guys dealing with security from an ICANN perspective, so you are focusing on DNSSECurity only or you are trying to cover a much larger scope to have end to end security for the Internet?

JOHN CRAIN: No, we focus on identifier security, not just DNS. We're not looking at end to end security. That's not us. We're not building security products. We're not looking deep in other people's infrastructure. We can't. That's not our role. Our role as mandated by our bylaws since the day we were founded is to worry about the security and stability, and we added resiliency because you need that when things really do break, of the identifier systems of which DNS is one. It's an important one, but it's only one.

HAMZA MEHREZ: Hamza Mehrez from Tunisia. I have a question that may be related to end users' security online. My first question is do you think that end users should use the Internet anonymously? And the second question is what are your recommendations to the threats to the development of the Internet of Things?

JOHN CRAIN: Okay, so that's two separate questions. They should be able to have privacy. And anonymity, which I can never say because it's such a horrible word – anemone, which is the one out of the cartoon with the fish – that's a different issue. So from one side of me, I say, "Yes, you should be able to be anonymous." But the other side of me says, "Well, if you're attacking me, you're a criminal, whatever you are, I don't want you to be able to be anonymous." I want law enforcement through due process to have some way of going and finding you. Remember the due process part of that is very important.

I, myself, am conflicted on this because there are times when I want to be absolutely anonymous. When I'm watching Facebook from work, I don't want my boss to know it's me just browsing Facebook all day, but I also understand the other side of the argument. So it's not an easy question. If it was an easy question, we wouldn't be having all of these fights, etc.

And what was the second part of your question?

STEVE CONTE: The Internet of Things.

JOHN CRAIN: Oh, the Internet of Things. I have a worry about the Internet of things, and that's that they're all very cheap. The devices are cheap. They're not as secure as they should be. Internet of Things is a marketing term for putting all of your devices on the Internet, just like cyber security is a marketing term. There are lots of marketing terms thrown around, the Cloud. They're all marketing terms.

So am I worried? I play with devices at home all the time. My light switches, I can control from my phone. I've got cameras I can do. You can't do any of this from outside my house. I can't do it from here because I'm worried about the security aspects, but within a controlled network, I play with these things all the time.

Frankly, most of them are not very well-built, but it's new technology. Cars weren't very well-built when they first came out, so a lot of this stuff, it's small, it's cheaper. Things will get better, I hope.

STEVE CONTE: [Inaudible] to that too, if I could. It's all right. I got a mic. The first question you had. Yeah, we work at ICANN and we have a very narrow and specific focus on what we look at with security, stability and resiliency. End to end user or end to end connectivity is not really within the ICANN remit, but let's be

honest. We're all end users, so we all have our own personal concerns and we try to balance that between my personal concerns and my work concerns and things like that.

There's some overlap on that, but John hit it on the head. It's not really where the ICANN remit is. If we go out of scope of where ICANN should be, then we're in territory that other experts are looking at. Collaborating with them is one thing, and stepping on their toes is another thing. So we try to collaborate with those groups when it's relevant to do so.

For the Internet of Things, I think what we're seeing is a period of rapid development of product. With rapid development, it's driven by the market share more than it is about stability and connectivity and security and all of that too. Everybody is so hip and excited about this Internet of Things. They're ignoring a lot of the, albeit old and albeit slow, process of proper protocol development through the ITF, which has check safes for security for protocol development. People just want to get this stuff out.

Sometimes it's great. There are some good services out there and some good Internet of Things things, but going through the process and understanding that if you sidestep some of that stuff, it's going to cause some issues. The more and more stuff we get on the Internet of Things, it's going to start compounding that.

We're starting to look at it from some aspects. Rick's doing some of the work on the DNS stuff of some of the IoT stuff. We're starting to look at it and dip our toes in the pool to see if there is something that's within the ICANN focus, but right now, we're just watching it as individuals.

JOHN CRAIN: Yeah, and if you look at all of these devices, a lot of them have DNS servers on. They're all going to need IP addresses. Are those going to be some kind of private IP address? Is it going to be v6? There's a lot of questions that touch us, but it's not because it's this Internet of Things. It's because they're affecting our world.

Anyone? Which one? You moderate. Okay, who was first? Let's start with that one. He's got his microphone on. Go ahead. No, this guy.

UNIDENTIFIED MALE: [inaudible]

JOHN CRAIN: Yeah, right at the very end.

UNIDENTIFIED MALE: All right, thank you. Thanks a lot. I have this clarification on two [inaudible] from you. Where does the control of the

securitywhen you want to compare with government control? Because where the [inaudible]. I'm more interested in that, too. But with what happens when governments choose to control our security happens on the domain. I don't know at what point they do that.

I'll give an example. At some point, my country and [inaudible] is my name from Nigeria, by the way. At some point, I can't remember what was happening at that time, but [inaudible] period of time [inaudible] or 24 thereabout, there was no Internet. Everything, you can't log on to any domain at all. Phones were blocked. I'm not talking about the phone anyway, but the Internet, you can't log onto it. We can't log onto ICANN. You can't log on.

At what point do we see the securities? By the way, there's a [inaudible]. The [inaudible] is that the same person that is interested in blocking the website can be interested in compromising the security.

JOHN CRAIN: Governments do what governments do. You're talking about the Internet and not the identifier system. We've had cases where governments have decided to turn off the bandwidth for whatever they've done to cut off access. If we look at it, we say, "Is there any effect on our ecosystem?"

Just because something is not working in the country doesn't mean it's not working in the rest of the world. A lot of the time, the DNS and everything for everybody outside of that country, completely fine, at least if they've built their systems properly.

Governments do what governments do. It's nothing to do with us. Those are national political issues.

We've had cases where things like that happen and people say, "ICANN turned off this country," because press people say whatever they want. Nothing like that has ever happened. We've never had pressure from governments to take part in that. Although I suspect if we did, we'd just go, "Yeah, go away." Governments do what governments do. That's not really our realm.

What is interesting is we have a lot of governments participate in ICANN processes, and when they're here, they all love the Internet. Well, most of them. They're saying, "This is very important," and then occasionally, you see – and it's very occasionally – you see things like this happen where they'll cut access to the Internet, not always on purpose, by the way. I've seen a couple of times where they've accidentally done these things.

It's an interesting topic, but it's not really something that ICANN gets into. The GAC never gets into these kind of things. It's just not our realm.

[BOB]: Thank you. I wanted to ask what the public trust, issues of the public infrastructure. What future do you see between the future of the certificate authorities and the use of DNS-based authentication of named entities?

JOHN CRAIN: You're saying where is DNSSEC going forward. It's like anything. You need applications to build on top of it that people will use. Personally, I'd like at some point for DNSSEC to be ubiquitous and that people don't really think about it anymore. It's just the DNS is secure. That could take years.

The interesting thing is there are things coming along like DANE, which is an area of the IETF where they're putting services on top of the DNSSEC if you like, the ability to have your own certificates and then authenticate them in some way. If people start using things like that, and some people are experimenting with it, then having DNSSEC may have more benefits than just the authentication of your answers. That will be interesting, and that's starting.

The person you need to talk to – I can introduce you – is a gentleman called Dan York from ISOC who is all about measuring this stuff. We have a gentleman called Richard Lamb who is also all about measuring this stuff, but ISOC has a lot of details on how this is growing and are people starting to use DANE and other things that they can put on top of the DNSSEC.

If we don't build anything on top of it, if we don't use the tool, then it'll just muddle along. It's the same thing with IP version 6. If you don't have a reason to use it, people don't. They stick with what they know. The reason was that the sky fell and we ran out of v4, but all of the other things that v6 promised never really interested anybody.

I think you were next.

MUHAMMAD SHABBIR: Thank you. I am interested if you can tell us something about the techniques and tools you [imply] to ensure the identifier security. What are the techniques, if you can enlighten us about that? And for the record, this is Muhammad Shabbir from Pakistan.

JOHN CRAIN: The tools are very simple. Obviously, there is research, measuring what's going on out there, looking for differences.

But there's also something call threat intelligence, which is basically talking to people, being on security mailing lists, being on all of the places where all of the issues are talked about. These are basic things. There's nothing major.

We have some labs. For example, we have a lab where we're looking at how packets change as they go through middleware, things like your home routers, and firewalls, and VPNs. All of those things do stuff to the packets and the identifiers. We do research. We have a small research group.

Then the other thing we do is we interact with the community. We are constantly talking to people in the security community about what are you seeing. If there's a threat, they know to call us. If we look at some of the large botnets that have caused problems on the network but also affected the identifier system, they're a threat both because they can be used for DDoSing the system, but also, often, they register tens of thousands of names into the system that are only there for nefarious purposes, which we feel is a problem.

Most of those, we don't find those. That's not our area of expertise, but we do know the people whose area it is and they know us. A lot of being on top of the threats and seeing things coming is not about knowing everything yourself. It's about

having the right peer groups so that you could actually learn from other people.

I saw you. I'll come to you next. Okay, go ahead.

HASHIM NOUMAN: Hashim Nouman from Pakistan. What are you doing to stop CGNs?

JOHN CRAIN: Nothing. Carrier-grade NATs. Nothing. We are watching with bemusement.

STEVE CONTE: And a little bit of shakiness too on it.

JOHN CRAIN: Yeah, and a little bit of shakiness. Whether you use a carrier-grade NAT or you go with something like v6, which would be my preference, is a business decision. People are looking at this very much from a business perspective.

Now if you're on the side that's wanting to see what's happening for vulnerability detection, looking for bad actors, things like that, this large scale [NAT-ing] of addresses and the problems associated with logging this are problematic.

My personal worry about carrier-grade NATs is that people will invest, going down on this path, a lot of money – they're not cheap – and then they won't have, maybe for many years, any incentive to go to v6. If this comes to default, all the big ISPs say, "Well, carrier-grade NAT, because it's got all these cool features, is the way we go," for whatever business purpose sense that they've decided this. I worry about the effect on the v6 deployment and getting v6 out to the ends, etc. But these are business decisions so they're really hard to influence.

STEVE CONTE: Just to add to that a little bit, too, I totally agree with what John just said, but when you do CGN and things like that and even just plain NAT, you or your device are changing what the packet was meant to be in the first place. So you're already changing your true end to end connectivity just by putting a single NATin somewhere.

I recognize there's value to it. I've got a whole network. I've got NAT and I use it, but when you put NAT on NAT on NAT on NAT, then you break it that much more and that much more and that much more. They're not an ICANN issue but it is an issue that needs to be looked at. I'm sure there's other people out there who are looking at whether or not it is breaking things and at what level.

Like John said, it's a business decision. If an ISP decides to use CGN and it breaks their customer base, it's horrible for the customer. I agree, but it's not necessarily affecting the stability or the resiliency of the Internet as a whole. Unless for some bizarre, strange mass hallucination we decide to put CGN really at the core of the routing, then it really does become the customer's problem or the business's problem when things don't work. That's not a great answer, but that's where we are.

JOHN CRAIN: You also have to remember that whenever we step into areas that are gray for us, we get shot. We're very much pushed for stay within your bounds. So things like that, they're right in that gray area. We are involved in discussions because people come to us for our expertise, and we want to learn. But it's not going to be anything that ever ICANN would make a policy on or anything like that. It's not in that realm.

Did you have a comment on this or a question?

UNIDENTIFIED MALE: [inaudible] CGN?

JOHN CRAIN: Do you want to do that?

UNIDENTIFIED MALE: Do you know what NAT is? If you have a home router and you have one public IP address, the router turns that into multiple IP addresses? A carrier-grade NAT is that same thing but at, oddly enough, a carrier grade. It's at a cell phone company or a cable or ISP where, because of v4 depletion and exhaustion, they only have so many public IPs but they need to serve 1,000 times the customer base than what they have for public IPs. They're turning that into a large NAT in the beginning of their network.

JOHN CRAIN: Things like you keep the addresses for very short spans of time. Lease times are really short, and logging that much change is extremely hard, they say.

UNIDENTIFIED MALE: Size-wise intensive, too.

JOHN CRAIN: This gentleman in the back, I think.

UNIDENTIFIED MALE: He's the same guy.

JOHN CRAIN: Oh, you moved forward. Don't move.

[JOHN CHAND]: Hi, John from Fiji. Talking on DNS security, what are the imaging threats to the DNS? First question. And the second question is how do you deal with [dealers' ethics] on DNS servers?

JOHN CRAIN: You answered the first question with the second one. One of the biggest issues, in my opinion, is DDoS. We used to have a lot of problems with things like cache poisoning. There's less of that now through solutions. You look at these problems, you look for solutions. Buy-ins] and all the other servers did port randomization to make it harder to guess which port would be used.

I'm sorry if I'm going to get too technical here. It's hard not to on these things.

Then we had DNSSEC on top of that and the cache poisoning, the lying about DNS names has gone more on the background. There are still ways of doing it. It's not perfect. As we deploy DNSSEC, etc., it's getting better.

Who here has been DDoSed? Denial of Service attack, take your network down. It's really miserable. There's not much you can

do about it. You provision and provision more, which is expensive, and you have your ISPs upstream provision more and there's a little bit of filtering you can do.

But if somebody really wants to DDoS you, you're just going to be in pain. You've seen really large organizations get DDoSed that have the funds, billion dollar corporations that have the funds to buy infrastructure and they still get DDoSed.

It used to be that we were seeing a very large trend in the growth of the size of the individual DDoSes, and we're still seeing some of that. I have not looked at recent stats, but we have seen DDoSes in the half-terabyte range.

Who here has a half-terabyte of bandwidth to their network? Yeah, nobody. But now what we're seeing is we're seeing more and more smaller DDoSes. We're seeing them used for different types of criminal activity. A lot of the time, it was some of these big ones were really about political expression and the "I don't like you; I'm going to take you down" thing. But now we're seeing a lot of blackmail and things like that. We're seeing a lot of extortion through crime.

Because of DDoS, botnets, networks of compromised machines, to me, they're one of the big problems of the network and we've not found a good solution. Even when we know where they are, which there are ways we can do that –we do look at botnets

because we think they're a threat – even if we identify a machine that is compromised and is part of a botnet, there's not really much we can do about it. They're a victim, but we can't even fix their machine because that would be illegal.

The criminals can get away with this stuff because they don't care, but you can't actually, in most jurisdictions, go and repair somebody's machine without their explicit consent.

So when we did [Configure] which was years ago, we had the IP addresses and millions of machines that were infected, but all we could do was reach out to the ISPs and hopefully they'd go and do something. We couldn't actually do anything even though technically, we probably could because we have some pretty smart minds in the room. You sit there and go, "If we just did this, we could make the whole thing go away."

STEVE CONTE: But just remember the owner of the compromised machine isn't the bad guy. It's your mom.

JOHN CRAIN: Both morally and legally, it was like, yeah, it's not the right thing to do. So that's probably the biggest threat, I think, by far. We actually have a document that lists a bunch of various threats to the ecosystem, but many of the threats when people look at it,

they're actually towards the business side of it, not necessarily actual technology. But DDoS, by far the biggest threat at the moment.

UNIDENTIFIED MALE: [inaudible]

JOHN CRAIN: [Inaudible] look. That's him.

UNIDENTIFIED MALE: This is [inaudible] from the Gambia, second time fellow. My question, I would like to bring back the issue of Internet of Things. My question is, is Internet of Things really necessary? Do we need it? Because to me, I don't see any [inaudible] for inventing Internet of Things.

STEVE CONTE: Do you have a cell phone?

UNIDENTIFIED MALE: Yeah. Okay. Again, my second question is what are the policies? What are the rules or laws in place to be able to protect people with all the security challenges that we're facing? Because nowadays you don't even need those technical skills to be a

hacker because you have all those tools available online where you can go download for free. So anybody can hack. So what are the policies or rules in place to protect or at least save these programs, these softwares from easy access?

JOHN CRAIN: It's an open market. There are no real rules. There are laws. There are laws in every country. If you DDoS somebody to extort money from them, that's extortion. That's a crime in that country. The problem is the fact that most things are not in a country. The victim may be in a country, but everything crosses jurisdictions. There are conventions like the Budapest Convention and other conventions that law enforcement deal with these. These are not ICANN matters. We're not law enforcement. We're not governmental. Law enforcement and protection of society is really a government job, and they make the laws.

Now a lot of old laws, i.e. physical laws, you can actually use them for the Internet. Crime is crime for the most part. There are very few crimes that are really crimes computer to computer. There are very few crimes that are really cybercrimes. They're normally crimes against people or against assets, and there's lots of laws to deal with that.

Now, it's really hard to teach judges and lawyers and legislators to think like that and to understand these things. The Internet's pretty new. We got a long way to go, but that's not ICANN's job. That's a government job and people who advise governments.

Do we need the Internet of Things? Well, Steve asked you if you had a phone. That's a thing. It's on the Internet so you need that one piece of Internet of Things.

STEVE CONTE: Yeah, I asked you to think of the Internet of Things. I think it's just a way to model that. They needed a way to term the fact that there's now more devices than there are people on the Internet. Before, you had a computer in a family and your family of four or family of five would share that single computer, so you had more people who were using the Internet than there were devices. Now that's shifted. I think if you think about the Internet of Things just as a different way to think about how and what's on the Internet and take away the marketing aspect of it, then that's really what it is. It's just a rapid deployment of more devices that are on the Internet.

JOHN CRAIN: Yeah, and you can ask the question whether or not you want your light bulb to be able to be controlled by your phone.

Whether you need that? Need is a big word. You need food. You need water. You need some form of power probably, although you could probably live without it, so need is a big word. There is clearly a market. There are clearly good uses for Internet of Things.

So at my house, because I'm a geek and I play with these things, if there is a fire, my fire alarms will go off. We've all got that, but mine are actually connected to the network. So when they go off, what else happens? All of my lights in my house turn orange and come on because orange is a light band that will go through smoke. If they detect smoke, they can also vacate the house by using the air conditioning system to pull the smoke out.

Sometimes, things can be more intelligent and useful and actually have life-saving properties when they can talk to each other. It all goes wrong when the security fails, but there are very clear and useful uses of devices that when you connect them, they suddenly gain a whole new life.

If you think of a thermostat in a house, how many of you go up to your thermostat and change the temperature every time you think it needs adjusting? You go, "Oh yeah, I'll just leave it. It'll go down." Or you may go do it once or twice a week or once a day, depending on how hot it is. It'll be running at lots of times when it doesn't need to. That's wasting energy. If you look at

some of these learning thermostats that have algorithms that they can then get new ones and they can be programmed remotely, for example, my thermostat. I can sign up with my electricity company, which I have not because I don't trust them, to a program where when the temperature gets above a certain amount, my air conditioning temperature will turn up. So I won't be cooling as much. That's a real use. If you've got an entire city of people doing that, you're really making a difference to the ecosystem.

Need is a big word. I don't think we need any of these things. We don't need the Internet. Need. But boy, is it making life easier. We don't need mobile phones, but they're very convenient. We don't need thermostats that connect to the Internet. I've not managed to figure out what the reason for a refrigerator is that connects to the Internet, but people tell me there are. Or a toaster. But the market will drive that.

I think a lot of the gadgets will disappear over time, but I think some things will turn out to be extremely useful.

STEVE CONTE: John, the boss said two more questions, but you're chatty, so let's take one more question, then let them get out on time.

JOHN CRAIN: I'm not chatty. I just like to talk a lot. I'm going to take two and we'll do them short. We're going to take this gentleman first and then we'll take that gentleman afterwards because neither of them have asked.

ANAND RAJE: Anand Raje, fellow from India. We are seeing a really big transformation in Internet space as we are moving towards Internet of Things than IPv6 [inaudible] is going on. So your expert comment on where you think in ten years where we will be on Internet because now we see that root systems like European Open Root Server systems [inaudible] DNS is coming up. Then you are having anonymous systems keeping up like deep web and dark web. And the privacy issues are there. We are having driverless cars, so things are there.

So how you feel that after in these ten years where we are heading towards?

JOHN CRAIN: Well, I can't see the future, but I can comment on a couple of them and try to keep it quick so this gentleman has a chance. These other alternate DNS systems, if they can figure out a way to make them all communicate, that'd be cool. I don't think they're going to because we've been saying this for years. If they

all go their separate ways, there won't be the Internet. There will be Internets, and then maybe we won't be able to talk to each other. So we've got to find a way, if we go from Internet to Internets, to cross those borders. Because I'm not saying it's a bad or a good thing. I personally have problems with it. I like the idea that if I send an e-mail, it always goes to the same place. Maybe there's some technology that can solve that. People are working on that.

We don't know where the Internet's going to be ten years from now. New technologies come. New technologies go. Maybe the DNS won't even exist. Who here actually really uses, as a human, the DNS? Me and Steve, we're weird. You tend to mainly use things like search engines and apps. Maybe they're in the background, but it may be unimportant to the actual user, at which point, people will be less greedy and political about it because it won't have as much value. That may change, but only technology will drive it.

I'm going to let this gentleman.

UNIDENTIFIED MALE: [inaudible]

JOHN CRAIN: I'm going to let Steve answer whatever question it is.

[HAMAD USAMA]: [Hamad Usama] from Morocco. Welcome to Morocco. My question is about your future strategy in your new stability and resiliency and how we can implement it in the future. About the second information about Internet of Things, we organized the confidence of what Internet of Things in terms of [inaudible]. It was so interesting, but all human beings don't know why we need this. It's to [facilitate] our life or just to be with the new technology. Thanks.

JOHN CRAIN: I told you, you're answering it.

STEVE CONTE: So to answer the first question, ask John. Going back to the Internet of Things, I don't think it's a question of need or want anymore. If we look at the telephone system over the past 100 years, 120 years that it's been around, it's very much like the same Internet model where only if you had it. Then more people had it, and then suddenly everyone had to have it, and now you're carrying it in your pocket. That carrying it in your pocket is the Internet of Things part. So now we have Internet and we've had it for 25 years. Then more people got it, and then businesses decided to sell things on it. Now we're at the point where

everything talks on the Internet. It's not necessarily a question of us needing or wanting stuff anymore. It's like what John said. His system speaks to other devices which, therefore, makes his life better or safer or things like that.

They're always going to pitch the whole refrigerator with the TV on it and will automatically call the store for you, and that's not the Internet of Things. The Internet of Things are these tiny, little sensors that are working in conjunction to make someone or someone's' life better and more convenient. I think that's going to naturally happen. It doesn't necessarily need to have a moniker of, a label of the Internet of Things. Mankind works hard not to work. That's what we're doing. We're working hard so we don't have to work.

JOHN CRAIN: First question, strategy. When we talked about SSR strategy, we're about to publish a new document

STEVE CONTE: SSR strategy? The framework?

JOHN CRAIN: Yeah, the framework.

STEVE CONTE: Our framework, we have a new framework for SSR. It's going to be published on our website probably within the next month.

JOHN CRAIN: We have to publish how we're thinking strategically for the next years, and we do that pretty much every year. We look at what we think the emerging threats are, where we think we need to put our things, so you have to plan ahead.

STEVE CONTE: And then we ask the community to review that. It's a dual process. We say, "This is what we think we're going to be doing," and then we bring it to the community. We're going to have a community review scene. Ask me about reviews. Over the period of the next year and a half, we're going to be having talks with the community selected committee to determine whether or not a) that we're doing what we said we were going to do, but b) that what we were saying that we were going to do in our future strategy is the right thing to be doing.

JOHN CRAIN: To the gala or not.

UNIDENTIFIED FEMALE: Thank you very much. Like with all things, I like to offer up everybody's time so if you see either of these guys, please stop, ask them questions.

JOHN CRAIN: Look for people with funny hats. It's usually us.

UNIDENTIFIED FEMALE: So thank you very much for coming and everybody, to the gala and enjoy your evening. I will see you bright and early tomorrow morning and on time.

STEVE CONTE: Before everyone stands up, last statement. It has nothing to do with security and stability. It has everything to do with you guys. You guys are really the voice of the Internet, and the fact that you want to be here and not paid to be here says worlds. So hold onto that and be what you want to be and make the Internet what you want it to be because it's yours, it's ours. I applaud each of you for being here. Thank you.

[END OF TRANSCRIPTION]