ABU DHABI – At-Large APRALO Capacity Building Part 3
Monday, October 30, 2017 – 12:15 to 13:15 GST
ICANN60 | Abu Dhabi, United Arab Emirates

UNKNOWN SPEAKER: It's Monday, October 30th. Check, check. [AUDIO BREAK]

It is Monday, October 30, 2017. [AUDIO BREAK]

Check check. It's Monday, October 30, 2017 in Hall B, Section A, ALAC, for the At-Large APRALO Capacity Building Part 3. [AUDIO BREAK]

HOLLY RAICHE: I think we're ready to go. Today's session is on the dark web. It was one of the topics that was rated most highly valued by all of you that you want to hear about. We are very fortunate to have aside from the incoming chair, Rob, put your hand up, and Julie who is Vice-chair of SSAC. We have Jeff Bedser who is also SSAC, but -- do you want to be your company as well?

JEFF BEDSER: Yes, sure.

HOLLY RAICHE: iThreat Cyber Group. The guy knows all about the dark web. I know nothing about it and I'm going to shut up.

JEFF BEDSER: Thank you for the kind introduction, Holly. I'm glad my company's name scares you so much.

HOLLY RAICHE: It did.

JEFF BEDSER: So, thank you for having me here today. I'd like to give a quick presentation for you that's going to be the basics of the Dark Web, and the concepts around what the Dark Web is. I will not be giving you a primer on how to use it. I will not be giving you links on where to download the tools. I will take no responsibility for any criminal actions done based on anyone doing their own research after watching this presentation.

So, with that in mind, next slide please. I'm going to give you some warnings, and simply this. The Dark Web is designed to hide information and to hide conduct that people don't want governments and law enforcement to see or know exists. As I put there, it's filled with some pretty awful things. We're talking

human trafficking, narcotics, child exploitation, fire arms and weapons sales.

There's some pretty horrendous things, so before you do any exploration, ask yourself, number 1. Do I really want to see any of that? And, do I want to have any type of residue left on my computer showing that I'd done it that someone might detect? Because it's really some risky activities.

Next slide please, Meryl. You can go to the next slide as well, please. So just giving the basics of understanding what the under web is. Dark Web itself is kind of a nebulous term that applies to many different mediums that are not on the surface web or the internet that the ICANN community interacts with.

So, the surface web, or the internet as we all know is indexed content and it's based on DNS queries and a system that allows you to index and find content with ease along a very large subset, so I think the most reasonable estimates for the number of domains on the internet now is somewhere close to 360 million between the gTLD and the ccTLD space.

The Dark Web is basically something that runs underneath, as the graphic shows, the internet. This graphic is misleading and I apologize there, but it actually does a job relatively well. It would lead you to believe that the surface web is the tip of the

iceberg, as the analogy goes, and that everything underneath it is much larger. It's actually flipped. The dark web is very small compared to the internet itself. At any given time, there may be between the various tools, 20,000, 30,000 sites, as opposed to 360 million domains, so scale wise, it's not even comparable.

But there are different means. There's Tor, there's Freenet, there's I2P. And they're all different ways of getting to Deep Web and Dark Web contact. Deep Web is something that's not necessarily on one of those other systems. Deep Web basically was considered the unindexed internet. So, websites that have decided to block indexing sites such as Google and Yahoo and Bing and the search engines from indexing them or their credentials so you can't get anything behind the front page without having the credentials to go in and see what's behind it. And that's considered Deep Web.

And then Dark Web are these other platforms that are off of the internet. It's difficult to describe but they're all using IP addresses and they're all using routing based on IP addresses, but they are not using the DNS of the ICANN world to transact. You have to know where you're going. You have to know the address to get there, and you have to have specialized software to get there.

Next slide please. So, what do people use the Dark Net for? Well, there are some legitimate uses, and I'm sure people in this room may be familiar with Tor being used for secure communications and such. But it's used to circumvent government censorship. It's used to provide whistle blowers with protection, to anonymize their activities. And it's used to avoid monitoring. I know of many journalists in parts of the world that use Tor to communicate so they will not be arrested for publishing the content in their countries and their jurisdictions.

However, anything that can be used for good can also be used for evil, and some of the worse uses are, as I said earlier, illegal firearm sales, drugs, counterfeits, human trafficking, shelters for pedophile activities, hiring hitmen, hiring people to cause harm to systems and other people, and it's usually referred to as crime land for that reason, for those types of activities going on.

Next slide, please. So, the primary differences between the Dark Web and the Open Web, and the open web again being the internet we're all familiar with, is it requires special software to access. So you have to download the software to allow you to access the components of the Dark Web. It's resistant to indexing which means you really won't ever see a Google that

indexes the Dark Web because it's designed to not be easily indexed.

For example, in Tor, they use .onion addresses but a site might change its .onion address daily, so it's not easy to index and keep track of where things are. There are indices, but if you kind of think back to 1995, the way Yahoo worked, it was actually a list of all the websites and you had to go through the list and find the one you wanted and click on it. It wasn't actually a search function.

So there are some out there, but my experience has been most of the directories that are available on the Dark Web are usually 50% stale or outdated by the time you find them. Half the links are already gone and have moved on elsewhere.

All communications on Dark Web are encrypted and that's again by design to protect the users, whether it's for civil society or for criminal activities, they all want encryption. So, it's sometimes considered an internet within the internet and that's because it still runs on the same IP infrastructure run by the regional internet routing companies; however, it's not run with DNS.

Next slide please. So, the three major Dark Webs. The largest one most people of heard of is Tor, what's called the onion router, which is most of the focus of the presentation because

it's the largest. It's the most internet-like. It functions the closest to the internet of the three.

The Invisible Internet Project, or I2P, it's up and coming, it's a bit smaller, and it's more about the services for communication, such as instant messaging, email and websites.

And then, you have Freenet, which is primarily for distributed file sharing, and it offers communication means through it.

Next slide please. So, quickly, how does Tor work? When you download a Tor software package to your machine to join the Tor network, what you're basically doing is giving yourself a means to access Tor, but you're also then turning your machine over as an access point for other people to by anonymized while they're using Tor.

So, in this example, when Alice is Tor client, it will pick a random path to a destination server. It's basically routing through other people's computers who are running Tor. And as it routes through each step, that next hop loses the information about the previous hop. So as it's hopping through, each previous point in the destination is dropped, so by the time you get to Bob's computer on the far side, the only thing Bob's computer can see is the last hop it came from. It has no idea of the steps in between Alice and Bob.

Next slide please. So, first of all, this should be very clear to this group, .onion is not a new TLD. It is not an approved top level domain by the ICANN community. Most people in this building this week know that, but a very large amount of the internet population as a whole has no idea that .onion is not an ICANN accredited registry operated TLD.

But when you use Tor, what you can do is you can create .onion addresses and sites, and then they're basically hosted from your Tor software on your machine. They can only be accessed when using Tor and if any of you have ever used some resources for passive DNS data, such as the one that ISC used to have or Farsight currently sells, you can see traffic all the time of people putting onion addresses into their normal internet browser and trying to go to those sites, and of course, it doesn't work, unless you have a Tor plug-in in your browser, but that's a different story entirely.

ALI ALMESHAL: Sorry Jeff, so basically, these are accessible only if you are having the Tor application? As a gTLD, these are not visible to anybody else?

JEFF BEDSER: Right, it's only accessible within the Tor software installed on your machine.

ALI ALMESHAL: If I understand it right, it's creating a second internet other than the one we are using.

JEFF BEDSER: Right. If you consider the Tor software almost a specific browser that only browses a particular, smaller component of the internet.

ALI ALMESHAL: Okay.

JEFF BEDSER: Like if Internet Explorer or Chrome or Mozilla browse the internet, the Tor software allows you to browse just Tor. So, similar functions.

MARIO ALEMAN: Somebody else has a question.

JEFF BEDSER: I'm sorry, please.

UNKNOWN SPEAKER: Yeah, I think this is also in the context of the last June 28th blog post in the ICANN blog which also mentioned Dark Web. There was a protest from many NCUC members in the way in which ICANN put the language in that blog post and [inaudible] character. It goes, "Dark Web is factually part of Deep Web, which many people use it for [inaudible] purpose and other purpose, and also for linking it with criminal activities a bit problematic."

And on second level, there are a lot of things which is outside of the domain system. For example, if you are using Tor or even if you are using IP [inaudible], all these are not in our domain system, and using the term Dark Web as an opposite of open [inaudible] could be problematic because Open Web's opposite is Well-guarded Web. It's not the Dark Web. Many parts of the Deep Web is accessible through various other ways, and even known [inaudible] web is available in many [inaudible] website homes. It's all doubtful.

Using that as an opposite of Open Web is a very problematic proposition. I think it's not from the freedom of expression point

of view. This needs to be charactered. Maybe on the same line as the blog post's goal character.

MARIO ALEMAN: This is Mario for the records. I would just like to remind all participants to state your name before speaking for our transcription and the interpreters. Also to say bring your microphones when you're not using them, thank you.

JEFF BEDSER: Thank you for those comments. Another question?

SATISH BABU: My name is Satish Babu. I'm the chair of APRALO. I've been an open source enthusiast for many years and a Tor user on a daily basis for more than seven or eight years at least. I sympathize with what has been pointed out in the sense the positioning of Dark Web as an inherently negative thing.

It's not necessarily appropriate because many of us use it on a legitimate basis for day-to-day kind of stuff. Since we value our privacy, we like to ensure that nobody is kind of tracking our movement. So, I agree that there are many things, as you pointed out, that are negative, but it's not a good way to kind of

completely dismiss the Dark Web because it is a legitimate tool for many people. Thank you. [AUDIO BREAK]

JEFF BEDSER: Robert.

ROBERT GUERRA: This is Robert Guerra, also a member of the SSAC. With another hat on, I've been doing a lot of training in the past in regards to civil society using digital security tools, including stuff like Tor, and maybe just want to add a little element to what Jeff mentioned.

Tor is used for a variety of different things, and so Tor is a browser that can connect to the Tor network, but can also be used as a browser, and it's primarily promoted by a lot of organizations as a censorship circumvention given the way it receives content, is that if you want to access a site, so there's sites that are blocked here in the UAE if you just connect directly. But if you use the Tor, because it goes through relays, you can access that content. So that's primarily being promoted for that, so you can browse and the server that's sending you content doesn't know that it's you, and your ISP doesn't see that it's you. So, in that aspect, it gets around censorship.

The other aspect that Tor provides as well is that you can publish content and hide it, and that's the part that's dark. So, using the Tor browser, per se, has a lot of different functionality, one of which is to circumvent censorship. There's a publishing, which is the .onion addresses, and that's a little bit different, so if people are interested in knowing those differences, I'm happy to follow up with them later.

HOLLY RAICHE: Could I just stop everything here? We've only got a few more slides, and then he can take questions, but right now, can we just have the whole presentation and finish it, and then I'm sure there are lots of questions and I'm sure that Jeff would really be happy to answer any of them, okay? And a reminder -- I should have said Holly Raiche for the record -- please identify yourself first.

JEFF BEDSER: Those are all really good comments and appreciated. I'll finish the presentation and happy to have any more discussion in the group like I have. So, just finishing up with .onion, again there's no master database, such as a Google that gives you a list of all onion sites, and many of the domains are randomly generated

and generally for temporary purposes. They don't exist for a long time.

Next slide please. So, the realities when investigating activities in Dark Web communities and Dark Web systems is simply this: the network is designed to provide anonymity, which is great for civil society and it's also great for criminals. The best chance at finding and identifying someone in a Dark Web community is to bring them out to the Open Web to try and get an IP address or find out who they are.

Most transactions and financially, they don't take PayPal. They don't take Venmo. It's all cryptocurrency. So, you've got to get yourself some cryptocurrency to do the transactions.

You really have to be careful if you're actually on Dark Web to be keeping yourself as clean as possible with no signs you're leaving anything about who you are because you are basically, no matter whether you're using it for just your own purposes for private communication, you're in a community that would be very happy to get your information to use it to defraud you because you're running in a community that has a large criminal element. They feed off each other as well.

And I'm not saying that because you're using Tor you're a criminal; please understand. I'm just warning you, if you're

walking in a bad neighborhood, even if you really love the shop you're going to, you've got to be aware you're walking in a neighborhood that there might be criminals who know that you go to that shop.

And in the community, there's a very large cultural distrust of others. Think about that as well. You are using it to protect your information, to make sure you don't get tracked. That means you don't trust the people that you're interacting with to not track you. So, there's a very strong culture of distrust within the community; it involves various communities.

Next slide please. And just a quick review, and then we can go to the questions and comments and discussion. We spoke about the various web software and how Tor works. We talked about some resources, limitations and expectations when traversing the parts of the Dark Web.

So, next slide please. Happy to go into discussion and questions and comments now.

HOLLY RAICHE: First identify yourself and then question. Go ahead. Ladies first.

NARINE KHACHATRYAN: Narine Khachatryan, APRALO. Is there any estimation on how many users are using Tor on a global scale and the number of users of the Dark Web? Thank you very much.

HOLLY RAICHE: Before I talk to Evan, Rob would like to add some comments.

MARIO ALEMAN: This is Mario for the records. We have one person that just raised their hands, Sivasubramanian. Please.

HOLLY RAICHE: Sivas, can he answer the question first?

SIVASUBRAMANIAN MUTHUSAMY: Okay, he called my name. So, fine.

JEFF BEDSER: So, I don't have actual, real numbers, but I can say that -- for either the internet users or Tor, but it's a much smaller subset just like the size of the internet versus Tor, Tor is a very very small representation of the internet. Internet users is a far larger number than regular users of Tor. It's proportionate.

HOLLY RAICHE: Do you have a follow up question?

NARINE KHACHATRYAN: Is there any estimation, like a percentage of the users, global users?

JEFF BEDSER: There probably is. I'm just not familiar with it.

HOLLY RAICHE: Rod, did you want to go ahead?

ROD RASMUSSEN: Sure, I just wanted to add a few comments -- this is Rod Rasmussen -- to Jeff's presentation here. Thank you, Jeff, for boiling this down to just a few minutes. It's hard to do. There's a few points of clarity I wanted to add to the presentation that Jeff just gave, just because I saw some questions, it looked like -- that people had on that.

One thing is that these various technologies use the same exact physical internet connections. It's no different, the bits and bytes going over the wires are the same ones that we use for the internet. It's a different protocol. It talks on different, as we call them, ports. So, just like the DNS is set up on certain ports to

resolve domains. You ask a query across that into a server, it gives you a response back, tells you an address to go to. These networks are basically the same, but there's just a different protocol being used.

The encryption means you can't read what's going on, but ISPs can see the traffic that is happening. So I think people can block Tor and other things, and do. These technologies are constantly evolving because people are responding to their use, whether it's a government or an ISP or what have you. So that's something to keep in mind when dealing with the actual protocols and the way they get implemented change overtime in response to measures and counter measures.

.Onion, while not an ICANN reserved name, is reserved by the IETF, and this gets into a whole different area of who controls name space and things like that, but it's a topic for a different discussion. It's just something to keep in mind, that .onion has been reserved for this other protocol, yet people plug it into their browsers thinking it's DNS and thus we get a lot of traffic in .onion in the DNS.

A couple of last points that I wanted to make are that law enforcement actually is getting pretty good at tracking down these sites on the dark web that are doing the bad stuff, so to speak. The child abuse things, the weapon sales and things like

that. And what's happened because of this whole way of distrust that Jeff was mentioning is that law enforcement has gotten smart enough to actually, when they find one of these, to take it over and then work to find who actually is connecting with these things.

Now, because of the way those protocols work, it's really hard to trace them back, so to speak, but they are figuring out how to provide basic fake transactions and things like that to break up these large scale criminal rings, so there's a lot of that going on.

Then there's a lot of, my last comment, inter-scene warfare. In other words, the bad guys are going after the bad guys a lot. So, the one will take over another forum, website, and things like that. It's almost like being in a battlefield, being there when you're dealing with some of this stuff. So that adds to the layer of distrust. Those are comments I just wanted to add to that excellent presentation. Thanks.

HOLLY RAICHE: Sivas, now go ahead. Thank you.

SIVASUBRAMANIAN MUTHUSAMY: I'm Sivasubramanian from ISOC India Chennai ALS. There are good and bad sides of Dark Web, as you presented, and the

bad sides are extremely bad, like child pornography, and human trafficking, and counterfeit, and hiring a hitman and so on. But the other side is a good side which is a required side, protecting whistleblowers and escaping censorship, and so on.

As a person who is on the policy side, would you [inaudible] Dark Web? Would you [inaudible] Dark Web? Would you preserve Dark Web? Or would you like it to go completely? And the second question is, these are all known sides of the Dark Web. You know Tor, you know that people connect through Tor and the 30,000 websites that you talked about are relatively known for the law enforcement agencies and others. Is there any other Dark Web still unknown, [inaudible] extreme criminals connecting with each other?

JEFF BEDSER: So, I would disagree that law enforcement knows most of the Dark Net sites. Primarily, I would say that is because it's almost unknowable because it moves too quickly. They expire quickly, they move quickly. They transact, they move on because they are trying to hide themselves from enforcement. And I do a lot of law enforcement training for international law enforcement and usually, I'm still training on DNS investigations, but they ask me about Dark Net and I explain it to them.

And when I say the size is 30,000, because when you calculate out the movement, and the changing and the indexes that are existing, that's a rough number that comes out. I'm very confident there's a large number that are out there that are not well-known by anyone outside of the groups using them. Because you can set them up in a way that if you're not publicizing them to a group to bring people in, no one is going to find them except for the people involved in doing it.

So I'm sure there's a very large component that's not known to law enforcement or even other criminals. They're protecting their own markets from other criminals, so they're not going to share. I think that was most of the answers, just the policies. So would I want to get rid of it? No. I'll give you an explanation of why I say no.

You may have heard in the United States a couple of months ago, there was a hate group, a white supremacist group called Daily Stormer. They ran DailyStormer.org. And after an act, a large protest, a young woman died during a protest, many registries and registrars started doing the chase of shutting them down, the DNS provider shutting this DailyStormer.org down.

Daily Stormer then said, "Well, we're going to move on to the dark net." I said, "That's great. Go ahead." Because the main point of an extremist group is recruitment. And, if it's so hard to

find and you're going from all the users of the internet community down to just people who use the Dark Net, your recruitment efforts are going to plummet. So, please, give them a place to go. That's great.

ROD RASMUSSEN: Just to add a comment. It really doesn't matter what we or anybody thinks about it. It's a tool and people keep creating them. To answer the other question he had, that's what goes on. People create new ones. There's all kinds of private ones that people set up because it's easy enough to do with various tools to create your own kind of little mini-dark web that may turn out to be a big one if it's popular enough. So these things pop-up all the time. But, it's a tool, just like all the other tools we have and it's use of protocols. We've got all kinds of hands around it.

HOLLY RAICHE: Actually, we've now got a queue; starting off with Robert. You're next. Or Evan, Evan was next. Then you're next. The gentleman in the back is after that. So we've got at least four. Satish, you'll be five. Go ahead, Robert. Go ahead.

ROBERT GUERRA: So, I just wanted to add a couple things too. Actually, I've known the people who developed Tor and so one of the ways that they were promoting it initially was the tool that everyone can use. They were actually promoting it to law enforcement as well because law enforcement, when they want to do investigation of websites, they don't want to appear on their logs as FBI is accessing your site.

So, a way that they were very successful initially was, it's a tool for anyone, but particularly if it's a tool that can be used by anyone and there's value by both, that's a way that it doesn't necessarily get shot down by anyone. So, they were using it if they wanted to investigate the same type of groups that Jeff was mentioning, and so that way that they can be anonymous.

A lot of the content, it was used for copyright infringement, putting content online, but something that one has to think about, and again, not wanting to get into too much of the technicality of it, is the one thing that it shares also with the internet is the importance of two things: understanding how the infrastructure is built and the importance of standards.

So the thing for the Dark Web, at least particularly Tor, it relies that there is a relay network and that you relay your messages through. So the assumption by a lot of users of the Dark Web, or want to use it for circumvention is that those relays are going to

follow and they're going to be protecting stuff. But there are criminal networks that set up and run relay networks, and there's also government entities that run it.

So, if you're wanting to use this for circumvention purposes, be aware, just like when you connect to the internet, if you don't know what the ISP is doing with your data or your registrar and they could be selling it, it's the same thing for this network, and so if you don't know that, you may have an assumption that you are being private and secure and anonymous, but there have been reports, I think Snowden's Revelations and others that intelligence agencies were running their relay networks, so they were actually then collecting all the details.

So, for any technology it's really important to understand the protocols and how it works, so if you want to be safe, don't assume anything. And this is for the good guys and the bad guys as well.

HOLLY RAICHE: Thanks. I don't think, Jeff, you have to reply to that. I think that was excellent. Thank you. You're next, and then Evan and the new.

JAHANGIR HOSSAIN: Hello, I'm Jahangir Hossain from the community [inaudible] Bangladesh. I'm [inaudible] in Bangladesh. Recently, just a few weeks ago in our country, there was a case. A couple of people came and explained. This name was Blue Whale. The thing is a couple of people killed themselves by playing the games and all media published the information, all the newspapers, that we issued a block and we should identify what they are playing.

As an important point of view, we got all his messages from the regulator to block [inaudible] of this, which is [inaudible] authority. Then it comes to stop the Blue Whale. And on my side we face the challenge of how do I get the information. We don't know. Even now, we don't trace the information. Even though our regulator has given us a certain time to block this, if we are unable to block then we can sell the license as well.

Because of the demand of the general public and the users, they're playing these games very interactively and those who identified they're playing the game, they gave us some interviews to some newspaper as well. It's really [inaudible], but they informed that in some of the web they got the link and downloaded the games. They are bound to play the games after a couple of days.

And we told the government authority that we can't trace this. Even the link, when we identified a couple of users through the media, how you get the link, how you get the information? Even more, we got them all, we can't trace. I asked Bob how to resolve this considering the operative point of view. Thank you.

JEFF BEDSER: So your belief is the link to the game came from, potentially, a Dark Web source? That got in their hands?

JAHANGIR HOSSAIN: Actually, we searched online. We searched the Open -- www, Wide World Web; we can't find and trace the information. Even if it will be something, an application [inaudible] and the application inside them to the Dark Web might be and [inaudible] I don't know. But we can't trace the information. But we found that in social media and other websites, there's this publishing that started from Russia, some of the players.

JEFF BEDSER: I think that particular -- and I'm not extremely familiar with that particular game, but I've read about it a bit. I believe that the links were always social media based. They were always fed through social media, which is almost it's own under web when

you think about it. It's a contained environment where you can have a link within the social media software that doesn't go out to the DNS.

So, I think that that's probably one of the reasons why the link wasn't found on the Open Web, is because it was probably social media contained. Which again, it functions very similarly to the Dark Web; it's a contained environment where everything you deal with is in one place. I think WhatsApp or SnapChat or one of those for example could do that.

HOLLY RAICHE: Evan.

EVAN LEIBOVITCH: Thanks. Evan Leibovitch, NARALO. Is it possible -- this is in the cleaning up rumors part of this; is it possible for an ISP that an end user is using, while they can't tell where you're going or what you're saying, is the ISP capable of at least knowing that you are trying to access the Dark Web by using a Tor browser?

And if that's the case, does your mere use of the protocols have a risk of getting you on some kind of watch list of somebody that could be a person of interest, even though nobody knows what you're doing with it?

JEFF BEDSER: I think it's fair to say yes. That probably has a lot to do with the jurisdiction you reside in, whether your ISP would or wouldn't want to do that. But the protocols coming out are on different ports and are traceable. Those are the protocols coming out through their ISPs so if they're looking for it, they can find it, and then they can know which IP within their own network it came from, and thus they can know which user was assigned that IP. So yes.

EVAN LEIBOVITCH: So they don't know what you're doing with it, but they might infer, "Oh, you're using it. You must have something to hide," and therefore you get red flagged. I don't know. I'm just wondering if that's the case.

JEFF BEDSER: I think the answer is yes because also, there are places where VPNs are blocked for that same reason. They don't want you using VPNs because they don't want you to have tunnels that do get tracked to activities they're not aware of and can't see. There are parts of the world where that happens, so I think the same thing applies for Tor and Dark Web.

HOLLY RAICHE: Could you talk into a mic, because this is being recorded?

UNKNOWN SPEAKER: Hi, this is [inaudible] and I'm from The Internet Society, Pakistan. You mentioned that the law enforcement agencies are looking into this and have been looking into it for a long time, and there was a very famous case of [inaudible] law enforcement agencies were able to catch the guy.

My question is, is there any global statement or policy, law, anything that can guide the other nations about how to deal with it in terms of law, and is there any joint effort in your organization that actually looks into it or a global force? Anything on a global level that at least denounces the use of Dark Web or anything?

JEFF BEDSER: I'm not aware of any global policy. I think the largest hurdle that the law enforcement and governments have to deal with is establishing jurisdiction. So, the largest one probably most of you have heard of is the Silk Road Takedown. The Silk Road is a large Dark Net site, but what the criminals learned was when you start congregating and getting large and getting a lot of

attention, that means law enforcement finds you and shuts you down. So, they've splintered. Now there's a bunch of much smaller, specific markets that are harder to find. It's more difficult for law enforcement to target.

But also, establishing jurisdiction is relatively simple with DNS. You do a geolocation on an IP address and say, "Okay that's within a country that I have jurisdiction for." With Tor, the person doing the activities may well be within a country that your jurisdiction's law enforcement, but all the traffic and activity you get has been through Tor so it's from IP addresses from parts of the world that are outside of your jurisdiction.

So, I don't know of any global policy. I know that there's conversations starting. I don't know where we've advanced yet, unless Robert, are you aware of any? Any global government regulatory things going on for regulating Dark Net use and such?

ROBERT GUERRA: There's a lot of different elements to that. I mean, there are parts of the world where the use of encryption requires okay by the government. So there's parts to Evan's point that the mere use of tools does flag you. Whether they choose to go after you is another thing, but they will use that including tax stuff, and so if they can't nail you on any other charge, they'll nail you in

regards to that. There have been talks at a global level by a variety of countries weakening encryption and making tools like this that can't be used, and so there were efforts in the UK I think to weaken encryption and stuff like that.

So I don't think there's a coordinated effort, and I think the larger question is, in terms of a dark web, it is being used by many in government to advance their agendas, and the issue is always, do they understand that, to your point is, the underlying technologies used here also underpin financial sectors, as well?

So, the issue is if you try to stop the Dark Web and make sure those technologies don't work, you may have the unintended consequence of having banking being insecure as well. So, it's a challenge, but that's why it's important to understand that the technologies are no different. I think there are efforts, but it's for a variety of reasons. Not directly but indirect ways of trying to control and tame it.

HOLLY RAICHE: Thanks, Robert. Floyd, you had a question?

MARIO ALEMAN: Holly, excuse me, we have one question beforehand. Yes, there is actually a question on the AC room.

HOLLY RAICHE: That is tiny. Could you read that out please?

MARIO ALEMAN: It is actually for Sivas, so he could go ahead and just read his question, thank you.

SIVASUBRAMANIAN MUTHUSAMY: No, you answered my question about whether you would encourage Dark Web or at least allow it to survive by giving me a sort of wrong reason to do that. That is to push the criminals away from the larger internet to a smaller corner.

Apart from that, my question was actually for good reasons, for the good of the Dark web. There is some good in Dark Web. For those reasons, would you encourage or at least tolerate Dark Web? That was the supplementary question. And there's another question. I've heard a friend mention something like the internet underground and the way she mentioned it, it was like brilliant technical experts operating in anonymity. It sounded more like a good side of the internet. Is there something like an internet underground?

JEFF BEDSER: I don't want to spend too much time being philosophical, but this is much the yin and yang of the internet. We can say that automobiles have been a wonderful product to help advance society and industry and gives us all freedoms to move about, but there's also people die in traffic fatalities, there's the pollution that comes as a side effect, and there's traffic which I'm sure none of us enjoy.

So, the internet has a lot of abuse and gives us all a career, I guess, to a certain extent. So, there's good and bad. You can use a firearm to protect yourself, or you can use a firearm to kill someone and to murder. So, should it exist? Yes. Should we all be aware that it's being used for some very bad things? Yes. Can you use it for good? Yes. When you're using it for good, should you be aware of what else it's used for? I think you should.

HOLLY RAICHE: There are at least two more people. There's Fuad, Satish put his hand up again, and I think there's one person over there. So, if you could all be fairly brief, because we have only 15 minutes. Thank you.

FOUAD BAJWA: Jeff, Fouad Bajwa. My question is, from the history of the internet, when it's related that the DARPA project was split into

two, one became the internet that we publicly use and DARPA was meant for military use. So, that sort of seems like the initial Dark kind of Web was created for their operations alone, right? For military operations alone.

And even before the World Wide Web caught on, I used to work for a technology company. We used to build off disconnected collaboration systems for the US universities and military research companies. So even those, there were these kinds of networks that were always there. My question is, is it just because of the illegal activities that these became so famous?

JEFF BEDSER: I believe so. I know that Tor's origins are very similar to, as you said, ARPA net, wherein Tor was designed to be a communications network [CROSSTALK].

FOUAD BAJWA: Tor was originally, I think, conceived by a naval officer.

JEFF BEDSER: Yeah. US Navy, yeah. And it was designed to be a backup form of communication where inter-connected computers could route traffic when other forms might have been knocked out in a military action. It was a redundant system by design in its

original concept. It can evolve to something else, but it's one of those areas where it's referred to as Dark, not because it's hidden, or maybe it is because it's hidden.

ROD RASMUSSEN: The question was about fame or infamy, right? I would say that we're here having this session because marketing departments at various security companies have been very good about hyping the threats of the dark web. That's kind of the reality of why everybody is interested in it right now.

The term dark web has been around for a while and its kind of evolved over time. And it's basically the stuff you don't see and the index thing is where everything gets -- that's deep web, yes I know, and all that. But it's this amorphous term which the marketing folks have jumped on to and now we have credit agencies in the US are advertising, "We'll monitor the Dark Web for you and see if your social security number appears." And scared scared, buy, buy, buy

So, that's what we're facing. So, I think part of one of the things that we want to do here today is remove some of that FUD; fear, uncertainty and doubt, around this, and just explain what it is. It's a tool, and unfortunately as any tool, as Jeff's been saying, can be used for good or evil.

HOLLY RAICHE: Satish, you had your hand up?

SATISH BABU: Thank you, Holly. Satish Babu for the record. A few comments. First is the fact that the US Navy developed Tor. Today it's an open-source project. Anybody can download and can make minor modifications and then restart something else, so I don't think it's really for us to stop such a thing. It's very difficult to stop.

Is it very bad? I think [inaudible] is much less. I've seen both. But I think [inaudible] sites that are much worse than what you can do with Tor also. So, at least Tor as she was saying, pushes some of these dark things to a corner and [inaudible] open it up for children, for example. So in a way, that is good.

Also, an abstract question, like is Bitcoin good? It's not easy to answer that. It may be good. It may be bad, so it's for us to use it. Secondly, Tor is actually a platform. You can make it a proxy. There are tools to push files, not just the web. It's a Dark Web. It's implies a browser. But Tor is beyond that. It's actually a platform proxy. It is not secure, as has been pointed out.

There's a lot of risk, traffic information attacks, other kinds of attacks. People have already started breaking Tor. It's not been breached in a large scale, but [inaudible] law enforcement can track it. I'm aware that law enforcement is tracking extensively the exit nodes. An exit node is a clear text traffic. And even in India -- in fact, I was asked to make a presentation to the law enforcement in Delhi about the Dark Net, and their idea was that they were going to start, at least one or two exit nodes so that they could see the end unencrypted traffic.

So, thank you for the excellent presentation because demystifies some of the [inaudible] of this topic and it is just a tool like any other tool. It can be used positively and people are using it. If you look at statistics on the countries, US is the largest. Germany, Netherlands, France, Iran is the only [inaudible] out in that list. So you can see what it is being used for. Thank you very much.

HOLLY RAICHE: Thank you, Satish. And I think we can wrap up, unless -- does anyone have any further questions or -- oh, Narine, go ahead.

NARINE KHACHATRYAN: Narine speaking. Is Tor, as a project, registered in any jurisdiction? And if yes, does it have employees and which countries do they live in?

ROBERT GUERRA: So, the Tor Project is a 501c3 Not-for-profit organization, much like ICANN. I think it's based in another state. I think it's in Massachusetts. I think it's based in Boston. It has staff based in the US and in multiple jurisdictions. Most of the Tor developers these days are based in Germany, but it's a distributed network, like many software development networks.

But it doesn't just develop Tor. Another project, it is open-source kind of tools as well, they also developed something called UniProbe, and UniProbe is a censorship internet measurement device as well. Kind of competition to the RIPE Atlas Probe that helps create a repository that's data driven of websites that are blocked. So, if you look up OONI, you can look up your country and see reports of websites.

So, it's a group of programmers, of encryption and others that are helping people understand the use of technologies for privacy, but also data-driven as well. They have -- like I said, the origins are very interesting. The source of funding for the Tor project, which is possibly another question, is it gets the

majority of its funding from US government sources; particularly the State Department and the broadcast board of governors.

So it is a technology that -- there's a lot of history there now, so I'm happy to follow up with people, but much like ICANN, its origins comes from the military. Tor does as well. It doesn't mean that it's controlled by the military, it just means that there was an interest to do that as well too. So, it's an interesting story, but to your point, Jeff, it's not the only Dark Web tool, and given how it works, a lot of law enforcement, but particularly law enforcement and intelligence, if it's an open standard, which is good, so you know how it works, you can also develop search engines that search the Dark web.

And so there are Google-like equivalents for the Dark Web that isn't accessible to all, that may not let you see where it is, but will let you save the content as well too, so as I was saying earlier, it's important to understand the technology, to understand that if people want to use it, be aware that it may have -- you know, as with anything in life, don't make assumptions that it's secure, private. There may be ways around it.

But there is a lot of activity that's there and understanding what the Dark Web is, who's using it, and the numbers is particularly important. It's not a loose term. It's an activity that doesn't use

a magical protocol. It's using the same thing we are using now. Thank you.

HOLLY RAICHE: Thank you. Now, before we let Jeff go, just a reminder for all of the participants, we are going to have a session with Ariel who has graciously agreed to walk us through the policy process and how you contribute to policy just after the session. So, you're allowed three minutes, that's it.

But in the meantime, I would really like to thank Jeff, and Rod, and Robert for their expertise, and if people have further questions, can they send them to either of you?

ROBERT GUERRA: Yeah, that's fine.

HOLLY RAICHE: Okay, I will make sure that we have email addresses, so if you have any further questions, we'd be happy to take them and we'll get answers for you. But could we thank our guests? Thank you very much.

ARIEL LIANG: Just very quickly, this is Ariel Liang speaking. Housekeeping, if you are interested in learning about the policy advice development process, the location is Capital Suite 1; that's upstairs. But simultaneously, there's a Cross-Community Session, so if you want to go there, please feel free. Make your choice. Thank you.

[END OF TRANSCRIPTION]