FINISHED FILE

ASIA PACIFIC REGION INTERNET GOVERNANCE FORUM
TAIPEI 2016
A NEW INTERNET ERA

JULY 29, 2016
ROOM 401
11:00 A.M.
MERGER 5
CYBERSECURITY THREATS POSSIBLE COLLABORATION
IN SOUTH AND SOUTH EAST ASIA

Services provided by:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
800-825-5234
www.captionfirst.com

***

***

>> BABU RAM ARYAL: Good morning. We have already listened to many people. And we'll stop by this. So, this is Babu Ram Aryal, from the civil society. By profession, I'm a lawyer. And there's supposed to be two -- but some technical difficulties. This is not -- and we are focusing on southeastern issues of cybersecurity. Let me introduce my esteemed panel, Mr. Arun Sukumar has just arrived on my right-hand side. He has a very good understanding on cybersecurity issues. By profession, or by education, he's also a lawyer. He's a good lawyer, I know.

And he has a good understanding of international affairs as well, because he studied international affairs as well. So, he is the Head of Cybersecurity and Initiative of Observer in India, and all of us who have elected him as Vice Chair of this APrIGF, as well. This is myself, Babu Ram Aryal. I already said I'm a lawyer by profession, and have served with various institutions. Internet Society, Nepal chapter. And I'm also an expert member of the National ICT Council of the Government of Nepal, chaired by the Prime Minister himself.

And we have another civil speaker, Mr. Jahangir Hussain, from Bangladesh. He's remotely participating in this conference. He has

a good understanding on network security issues. And he, by education, is a technical person. He has technical expertise of cybersecurity. Rohana is from Sri Lanka. He has a good understanding on how to handle incidents. He is a trainer as well. He has trained many national and international people who are directly involved in law enforcement issues, and first response on cyber attacks.

Said is from Afghanistan. This morning, he was just saying -- government. He represents civil society as well. He has experience from government side as well. And he was extensively involved in various government activities on cybersecurity issues, advising on the Cybercrime Bill, and other cybersecurity-related issues in Afghanistan. Subash Dhakal is from Nepal. He is leading new initiatives on a new law on technology in Nepal. And he is the lead who has established a government cloud in Nepal. And he is also working on setting up something for the government in Nepal.

Zakir, an understanding of results and practical advice. He has been participating at various national and international organizations like ICANN. He's a member of ISOC. And he's also serving as communication counsel. And he's part of the School of Internet Governance, correct? And he has a good understanding of internet governance and participating in various government issues, national and international. Just two days ago, there were Presidential policy directives passed that say cyber incidents are a fact of contemporary life, and significant cyber incidents are occurring with increasing frequency impacting public and private infrastructure located in the United States and abroad.

What I am referring is, this is a development from the office of the USA. And this establishes federal mechanisms to combat these cybersecurity incidents. We will be focusing on measuring the trend of cybersecurity issues in southeast Asia, what are the mechanism in south Asia, and what are the measure -- possible collaboration in south Asia. I thought it was going simultaneously. Can you see the numbers? Okay. So, Maldives is having highest penetration. It's around 58.5%. And Bangladesh is having 31%. Bhutan, another small country, is having 34%.

And other major countries are below or around 30%. Afghanistan, 12.3. And Nepal, 18%, around. Pakistan, 14%. And India, 30%. Though this penetration is -- this is scale, but, security threats are very huge in south Asia. Companies are working on content, and basically, threats are on content. So we'll discuss what are the level of threat, and what are the practices so far, government and private sector is doing to combat this. A few facts, again. Cybersecurity reports that 1 trillion will be spent globally on cybersecurity from 2017 to 2021.

It's not a small amount. It's a very huge amount to be spent. So, I'll start with Said Zazai from Afghanistan with a few questions. Is there any survey about cybersecurity incidents, or any cases you can say -- share with us, or any -- you have legislative framework,

and any collaborative approach you have? You can start your slides. I know you have prepared a very good presentation. Thank you.

>> SAID ZAZAI: All right. Thank you. Okay. So, to answer your questions, Babu, I have prepared some slides which will give you some introduction to the country, the infrastructure there, and the status of cybersecurity issues. Can I have the clicker? Okay. So, we're on the map pretty vividly for the past decade or two, but this map doesn't just tell you about our neighboring countries. We are at the edge of south Asia. Central Asia, and also the Middle East. So regionally, geographically, we consider ourselves pretty strategic.

And that is why we believe that collaboration among the different regions and within the region is pretty important. So our population is 31 million. We are the least-connected country in Asia Pacific. Even though we have a lot of improvements in the past 13 years, since 2001 and 2, but still, we are the least-developed -- least-connected country. ICT global ranking, according to 2015, is 156, down from 149 in 2013. Household internet access, according to the ministry, it's 6%. Slightly different than what Babu was referring to.

But, then again, you will come across these different statistics within Afghanistan. Broadband price is ridiculously high. 38.6% of GNI, fifth-most expensive in Asia Pacific. But according to the government, the prices are going down. But not for the past two years or so. So once again, just a map of the fiber optic connection to Afghanistan. We are a land-locked country, so we're highly dependent on connections through Pakistan and central Asian states, Iran. And we also have a border with China, but really high mountains.

And I think it's not really feasible to connect through China. But they have that in the government plans. The current connections that we have, we have two connections coming through Pakistan -- a connection from Iran, and two from Turkmenistan, but they're all not active. This is the plan from 2008 and '9, which has delayed, but we're highly dependent on the connection that is coming from Afghanistan. So, insurgence, cutting that fiber optic cable, sometimes our internet shuts down for hours or sometimes for a day or two days.

So if you guys are emailing me and I'm not responding, it's because the Taliban has, you know, put a bomb somewhere on the fiber optic connection. It's strange that the Taliban have found those cables under the ground. (Chuckling) Yeah. Sometimes the technical community, we believe that these are sometimes the operational issues when you call the operator, they say that it was an insurgency. So, this is the environment that we are in that affects the whole cybersecurity issues. Some of the major incidents we had -- I could only bring three examples.

There were a couple of bank incidents where the access was shared within the organization with a hacker. Was it sold or not, that's

unknown. But the amount that was stolen was $1.2 million, U.S. dollars. And the employee -- a female employee -- I don't want to target any gender, but in this case, it was a female employee and she disappeared to some other country. So the case is still pending. Another incident was with the government ministry. I don't want to name the ministry. It was an unauthorized access was given, was shared, or was stolen. And roughly 4 million U.S. dollars were transferred to a very -- a famous person in the country.

Again, I don't want to name their titles or anything. But these are the sort of incidents that occurred within Afghanistan. Even though we are like 6% internet access, the types of incidents and the scale of the incidents are as major as probably any other country. The third example is the attack, cyber attack, on the National Data Center, where all the government websites, .gov, and email, are hosted. It was some JavaScript attack on the websites, and all the servers were infected, and all the data was leaked.

Some of the challenges that we have that I could identify are -- they're mostly skill set-related, or software-related. The picture that you see on the right-hand side is typically the pirated software that is widely available in the market. Unfortunately, they come from our two neighboring countries in the east and the west, Pakistan and Iran. This particular example is of Iranian cracked software CD. In the right picture, you will see all the list of different vendor applications that are cracked with all sorts of malware. And the unfortunate thing is that all the government organization -- all the ministries, and independent directorates in Afghanistan, they use this software instead of licensed software.

So this is the beginning of what really happens to -- or why most of these incidents have occurred in the past. Most of the software are cracked software, or operating system usually not updated. They're out of date. Patches are not installed regularly. And when you talk to a security expert, they will tell you the first thing you should do is patch your software, update your software. Antivirus is not a trend in most of the government agencies. If the antivirus is there, it's not updated. If I could share one example of the ministry I was working at -- so they procure a number of -- like 1,000 or 12,000 licenses for antivirus software.

And in this particular case, the person who was in charge of the procurement within the IT directorate, he was purchasing the licensed software. And then he was installed the cracked software. And then he was going back to the market to sell it back for some cash. Unfortunate again. Kaspersky reported that something is used in the country which taps all the GSM network very easily. The skill set is another challenge that we have in Afghanistan. We do have a sort, the cyber incident response team. It was established -- I was expecting that.

It was established in 2009, but, like, you know, what most of us would be expected, if it's not dormant, it's not really active. I was telling Rohana it's highly inactive. So all the investment that it has gone in the past so many years for that, we're not utilizing that. And the reason for that is the skill set was just focused on one or two individuals. It was not given to the whole department. And we also have some organizational -- or management problems, the way they were tackling the employees, that was also a reason that skill set was not improving.

Another growing threat is the fact that Afghan cyber space is used as a proxy, a space were everyone can come in and do what they want and get out, and be happy. And the reason for that is, again, these software that are coming in, and all the -- whatever you call it, the malware, the bloatware that is used in using the Afghanistan IP addresses and servers, you know. It's pretty easy. There are also cross-border threats. These are from individual levels to the government level. This is also a threat that needs to be addressed through our regional collaboration.

So government has made some efforts in order to draft a cybercrime law. They have also drafted an e-transaction and e-signature law. And there was something established in 2009. But the laws that they have drafted are based on a convention. And like I said in the early morning session, one of the major articles in that law is that they are redefining the definition of minor. In the traditional law, a minor is anyone below 18 in Afghanistan. But what this cyber law, a minor is anyone below 16. So people from -- individuals between 16 to 18 are targeted. They can be criminalized, and they can be put in jail or fined with ridiculous amounts.

So these laws are still in draft. A public consultation has been done. No comments from the individuals or cyber -- sorry, the civil society has been considered. So just to conclude my presentation and to answer some of the question is that even though we consider that there needs to be a regional collaboration or cooperation, information exchange and all that, in the beginning, we also need a level of commitment and support from within the government, which is very minimum in our case, political and financial support from the government is minimum to the Ministry of Infrastructure, or the cybersecurity departments across government entities.

We also believe that there is -- there could be effective public pilot partnership within the country, because private sector is growing. There is a number of telecoms with large resource skills, and they could be utilized and their cooperation could be beneficial to government, because most of the infrastructure is -- if it's the fiber optic operator, the telecom, a regulator, they're government-owned, so that's why I put a lot of emphasis on the

government initiatives. Cybersecurity awareness within the country is low.

Because we have recently adopted internet in the past few years, cybersecurity awareness hasn't been done very effectively either from the government or from civil society, or academia. Regional exchange of information is needed in order to combat piracy. The software CD picture that I showed you. And also, to address the cross-border threats. There are some other exchange of information that we could do, which is the threat identification, and also in some of the mitigation methods, situation awareness, best practices exchange.

So these are the sort of things that we could do within south Asia. Collaboration on CIRT, where technical skills development could be achieved. Sometimes we have some procedural and organizational problems, and that could be shared -- in the case of Sri Lanka, and Rohana, they're vastly experienced comparing to Afghanistan. So probably what we could do is establish some sort of collaboration with them. And this could be from state to state, or CIRT to CIRT, or state to academia, probably in Sri Lanka or vice versa.

The final recommendation that I have is the -- and this is not the least, but the most important one, and that is the ethics of the IP security specialist. Usually, you saw the incidents that I shared with you. They were mostly by the individuals within the IT directorates or security engineers, so they had a huge influence on facilitating the incidence. We need to comply with the laws and regulations set by the industry. Also, they also need to consider the client protection. And client and customers could be different in this case. And the intellectual property copyright and data owners, and also not violate their own authority over systems.

So these are the sort of recommendations that I believe, you know, come under skill set or technical skills, organization skills that you need to establish our collaboration and cooperation. Thank you.

>> BABU RAM ARYAL: Thank you, Said. we know Afghanistan is facing a big problem with civil war and ongoing difficulties in fighting between -- among themselves. But we have a very good understanding that Afghanistan will come over with this, and will flourish in this IT sector. Before going another speaker, I have a couple of questions for you, Said. Do you have a law or a law of information covering data products and privacy issues? One question for you. Another question for you is whether private sector is also not that much aware.

Or what is the approach of private sector in Afghanistan about the data protection privacy, and these kind of cybersecurity attacks?

>> SAID ZAZAI: For data protection, we don't have any law for that. And as far as I know, there is no plans. Even though within

our civil society we have been raising our concerns over that. But we are a donor-funding country, you know. Whatever comes from the major donors, you know, whatever they call, we do that. (Chuckling) I mean -- government. So data protection has not been on the agenda for the donor agencies, unfortunately. And your second question was . . . Yeah, private sector, we do have a number of telecoms which are highly equipped, but they are highly closed doors, geared towards the government or towards other ICT service providers.

ICT service providers, however, they don't have that much capability and skill set available. But we also need to realize that they are growing, and they are establishing their skill set. And in the past -- particularly in the past couple of years or so -- our ICT sector has grown. And there's a number of startups and initiatives that are coming in. But they are not of the scale of where they can, you know, sit together with the government or the donor agencies, or the telecom and challenge some of the issues. But probably in a year or two, they will have that skill set ready and provide more contribution to the government.

>> BABU RAM ARYAL: Thank you, Said. We have two remote speakers as well, one from Bangladesh and another from Nepal. From Bangladesh, Jahangir is speaking. And from Nepal, someone is speaking. Before going to a remote participant, I'm going to another country, a neighboring country of Afghanistan and myself, Pakistan. Pakistan has some troubling issues in cybersecurity as well. They are currently drafting a cybercrime law, and there's huge debate on certain issues of the cybercrime bill. So, I'm going, again, with all those questions about the situation of cybersecurity incidents, and threats, level of threats and approaches, and training in Pakistan, and the approaches of private sector as well as government sector, from the legislative mechanism prospective.

I'd like to respect you to shed some light on possible collaboration depending on your experience. I know there are some issues with Indian -- and there are some allegations from India, some cybersecurity threats from Pakistan's side as well. I'll come as well in the next round. But, with this kind of experience, what will be your recommendation in this south Asian region now, Zakir?

>> ZAKIR SYED: This is Zakir, for the record, Zakir from Pakistan. Very interesting debate, actually, Babu, that in Pakistan, the law that Babu just mentioned, it's a draft. They are debating it. Interestingly, the day before yesterday, the Senate Standing Committee has given a green signal, and they are going to, you know, pass it, the Senate. And in Pakistan, we have a lower house called the National Assembly, and the upper is the Senate. The National Assembly approved it earlier, it was sent to the Senate, and there was a committee that had to review this draft.

With this said, we'll be in on collaboration with different stakeholders and reportedly, they have been saying they actually did

collaborate with different stakeholders. On the other hand, there are civil society organizations that actually still want to run certain amendments. But as of now, the Senate Standing Committee has actually given the green signal for passing that. Coming to the background of internet and cybersecurity, and the overall ecosystem, Pakistan probably is the most diverse market in terms of internet access and, you know, technologies -- not just within the region, but across the globe as well.

If you see, in Pakistan we have got a number of access technologies, for example, 50, or GSM, in Pakistan, in turn, had the world's largest WiMAX network. At time, it had the world's largest WiMAX network. And a couple of years back, they deployed the bonding, the 55 on traditional copper lines. They were the world's first demo. Then they actually demonstrated technology, 9.3. So they actually did take some revolutionary steps in the telecommunication industry, as long as the access -- you know, technology is concerned.

But on the policy, regulation, and legislation, this is a fact that Pakistan actually is a little behind. The draft that is currently in the Senate that is being discussed was actually -- I mean, they started working on it almost ten years back, in 2007. 2007 they started working on it. They are right now at a stage where they feel they are going to make it part of the law. So, the number that we saw on the slides as Babu mentioned was for the fixed broadband penetration in Pakistan, 14%, which right now is over 30% because of the introduction of 3G and wireless, cellular technology.

And it's still skyrocketing. So on the technology front, we are, like, evolving. But on the policy and regulations and, you know, on the legislation side of cybersecurity and internet policies, we still are far behind. And there is a huge gap in this. And this goal in internet access and penetration is actually giving rise to a number of different cybersecurity issues which include, you know, those from across the borders. I mean, this actually is for discussion. There have been instances of cybersecurity incidences, you know, originating from this part of the border targeting some installations there.

On the other hand, we have had incidences originating from the end and targeting. If countries like, for example, United States and China can sit together and they can, you know, discuss things on the cyber law and cybersecurity that they wouldn't allow their land to be used for originating some kind of cybersecurity threats from their land, and targeting, I believe that -- to be used for these kind of threats. And they recently had a similar kind of MOU with the Indian government as well. So I mean, these are very positive things coming in. And in south Asia, yes, definitely, the different markets and the governments within the region need to collaborate and corroborate so as to overcome this challenge of cybersecurity and stuff like that.

Coming to the background of cyber law in Pakistan, we initially had, you know, this electronic transaction act of 2002. I mean, that was kind of a strange situation when, you know, somebody is arrested for, you know, committing a telecommunication crime, or, you know, trafficking or IP. The ETL, the Electronic Transaction Act of 2003 is being applied in that situation. So because of the lack of the availability of cyber law to, you know, to tackle that particular situation. And then in 2007, they introduced this Electronic Data Protection Act that, again, had actually some additional things covered including hacking and data security, information security, and a number of other things.

But, you know, with the evolution and innovation in the telecom landscape, a number of interesting scenarios have been popping up. And there is always this need of revising and revitalizing rules and policies in cyber legislation. So, actually, in 2007, they realized the fact that we actually need some cyber law, and they started working on it. Right now they are at a point where this appears to be, you know -- they are so close to making it a law. But still, there are certain, you know, concerns from different segments from within the community, the local community, with the government.

And they are trying to discuss with them to get in their expert opinions and suggestions. Cybersecurity -- I personally believe, you know, on the technology front, things are evolving. On the technology front, we are evolving. On the policy side, it is sort of a multistakeholder scenario. I mean, every segment, every stakeholder from the community actually has to participate to be able to give rise to a cyber secure environment, and, you know, a cyber secure, maybe borders or community, or situations.

So in Pakistan, interestingly, I've got very, very active academia, the local community, the private sector, the regulatory authority. We've got an organization -- a local thing called National Response Center for cybercrime. They've been coming up with very innovative approaches. They recently introduced this initiative called Cyber (?) and go to colleges and universities and actually give training to youth to -- you know, to be able to make them realize the significance and importance of cybersecurity and protection in the online world and stuff like that.

>> BABU RAM ARYAL: A very short question for you, Zakir. What is the major alarming cyber incident trend in Pakistan?

>> ZAKIR SYED: Well, there have been a number of cybersecurity related incidences, which include, as you mentioned, some international -- you know, incidences originating from across the border and targeting some government installations. And within the country, there have been some attempts of hijacking, web applications and software and stuff like that. Interestingly, on social media as well. There are these statistics for -- I mean, the local side has

been receiving complaints on a monthly basis. They have been getting 300 or something hacking and spoofing and these kind of incidences.

But as long as major cybersecurity incidents, I think maybe we are still waiting for one to happen. And that is something they have realized and they are working on it with different stakeholders.

>> BABU RAM ARYAL: I expect a very quick answer again. What is the capacity of the law enforcement agency to handle cybersecurity incidents in Pakistan? Are they competent, or what is the position of the law enforcement agency to combat this?

>> ZAKIR SYED: As I mentioned, there was this lack of legislation. There was, for example, a particular -- I mean, there were a specific type of related incidents, and they had incidents, they arrest the culprits. But unfortunately, we didn't have the relevant laws for that. So, I mean, those were involved in those kind of activities, and released again.

>> BABU RAM ARYAL: Thank you, Zakir. Let's move to Bangladesh, Mr. Jahangir Hussain who is waiting and listening to us. And our next speaker is from Bangladesh, Mr. Jahangir Hussain. Is he online? Yeah, please.

>> JAHANGIR HUSSAIN: Thank you. Can you hear me?

>> BABU RAM ARYAL: Hi, can you hear me?

>> JAHANGIR HUSSAIN: Yes, I can hear you. Do you hear me?

>> BABU RAM ARYAL: Yeah. Thank you. Thank you for joining remotely from Bangladesh. If you are aware of our discussion, we have started with a position at the beginning. And could you please share some of Bangladesh's perspective on some of the issues that we have been talking about, very briefly?

>> JAHANGIR HUSSAIN: Yeah, sure. Thank you to all. I'm fortunate to participate in this session. I'm sorry to not be there in person. Right now the cybersecurity awareness and capacity-building is very much a growing concern in Bangladesh, especially the recent cyber attack in Bangladesh bank, where it was a $1 million heist. So, you know the situation in Bangladesh is really a terrible situation in cybersecurity. So, the government is now focusing on lots of issues, the capacity -- from the process. So, Bangladesh government -- the government is very for cybersecurity to bring cybercrime under some strict regulation, especially the last cyber attack in Bangladesh Bank.

A draft cybersecurity has already been prepared for final discussion, which is waiting for approval. So, right now at present, a couple of cyber law already in here, which is related to cybersecurity in Bangladesh. It is information and communication technology act 2006, another act of 2012, and Incident Provision Act, and Bangladesh Liberty Act 2011. And the most important things -- and the national cybersecurity strategy, from 2014, which is also related

to social cybercrime also, not only cybersecurity, but also social crime, especially on social media.

Those are related to social crime on media, then it's also on the security act 2015. So, right now this, already update, the security act 2016. And it has been placed for community approval. This act is coming at the version of cyber protection law of our country. And it will replace controversial position, cybersecurity law in section 57. Actually, section 57 is included a social crime in social media, or if anyone act illegal, it also -- the security act 2016. That's why there's a section that's very important for us. So, this is actually current law in our country, in Bangladesh.

Based on this, the last couple of years, there is government, private sector already -- local -- for local and regional collaboration for cybersecurity mechanisms and information. One of the special collaboration local is an incident response team which has published a project, LICT. Recently, there was full membership, for incidence response and security. The thing is, this year, government taking lots of initiative for cybersecurity awareness, build up capacity, which is a process and multistakeholder platform.

And another thought locally established is the private cert, and members maintain this cert and work with government. Can you please go to the next page? I think it is better for audience. Okay. I already talked about CIRT, it was recently formed to handle the government incidents. And one of them, another CIRT is already established in Bangladesh, is BD CIRT, the private one, but government probably work with them, which also member of AP CIRT. They are working in our country, and they especially take care the service provider side.

And another CIRT, just two months ago, was built. It is one of the busiest CIRT -- the Bangladesh Computer Security Incidence Response Team, and the military commission. This is actually one of the true multistakeholder platform or service provider, telecom sector, and other provider, and user directly involved for collaboration, for achieving the information mechanism locally and regionally. For building this up is actually -- is direct sector. So, internationally, especially the Bangladesh category.

You already know in media that there are $18 million heist from our country, so in Bangladesh situation, right now is to build capacity, implement security. So we need more discussion with you all to how we build platform by deploying multistakeholder platform to access information among us. This is one of the challenging from our country. And the government become more active, CIRT, so that we can share or get information from you how we collaboratively work with you for our country and our region. I think we can share and get comments from all of you, how to achieve this goal. Thank you.

>> BABU RAM ARYAL: Thank you. We have lots of thoughts. Still you have incidents.

>> JAHANGIR HUSSAIN: Yeah. After the Bangladesh Bank heist, $1 million, that's really everything for us.

>> BABU RAM ARYAL: You mean, just -- this mechanism, not that much strong from a capacity point of view, do you think?

>> JAHANGIR HUSSAIN: Actually, yeah. The thing is, the two CIRT is government-owned. Two or three months ago, they formed this CIRT. And one is private. They are working. But not so much active, because, you know, the working method of CIRT is permission. So that's why I need to share the challenges, how to collaborate locally and regionally to get the information, access to information. These are the important things.

>> BABU RAM ARYAL: Just this morning, we had one discussion on issues in southeast Asia. One of the participants said -- I should not say I was -- at least 24 bloggers were killed in Bangladesh, and the government is trying to come more freedom of expression issues. But what about cybersecurity issues, other kinds of threats other than freedom of expression? What is the approach of Bangladesh government from a legislative and practical point of view? Can you say these things very quickly?

>> JAHANGIR HUSSAIN: Yeah. The thing is, you know that this situation in Bangladesh with bloggers and other things, the government -- the security act which I already told you is under -- in 2016, which were 20 years of -- I think it was 12 years. They take 12 years. In the last 12 years, the cybersecurity law related to the act, now after that, they form 2016, the security form which directly -- a social crime, or blogger-related activity which is illegal, or someone acts, or someone illegal. So they are under law in the Security Act of 2016. So this is actually a place to improve.

After that, I think --

>> BABU RAM ARYAL: Thank you.

>> JAHANGIR HUSSAIN: Share the information. But, actually, things are not finalized yet. But this is an important year for our country, because lots of things are going on. And lots of policy are building, for litigation of cybersecurity.

>> BABU RAM ARYAL: Ladies and gentlemen, let's go to government approach. Let's explore what government understand about cybersecurity and what are their plans. Let's go to the Nepal, and Mr. Subash Dhakal, for the Department of IT, participating online remotely to this conference. He was there in Macao and Delhi personally, but because of some other issues, he's not able to join this in person. But he has been working on the cybersecurity issues in Nepal. Mr. Subhash, are you there? Can you hear me? Okay. He's not there? Okay. No?

So we'll come later on with him. Rohana, you also belong to government infrastructure. And listening to these guys, what is your

approach? With your perspective, can you engage more in this discussion, please?

>> ROHANA PALIAGURU: Shall I go through my presentation? Good morning, everybody. In this presentation, I will focus on the areas that we are going to discuss in this panel discussion. Before that, I need to give you an overview on what Sri Lanka is, and the culture. Thanks. Sri Lanka, I think, most of the Asian country, people know where Sri Lanka is. But, Sri Lanka is at the bottom of the -- in the Indian Ocean, at the bottom of India. The size of Sri Lanka is around 26,000 kilometers. And our population is around 21 million.

These are some of the resources and beauties in Sri Lanka. Sri Lanka is very popular for something, and we have a nice environment. We have resources like gems. And our popular game is cricket. Even though it is not the national game, the popular game is cricket. We have nice beaches and spicy food. If you love spicy food, you may come to Sri Lanka. And I will talk a little bit about where I work, Sri Lanka CERT. In early 2003, we started an initiative called in Sri Lanka, with the support of the bank.

And as a result, there was a lot of development in the IT sector. As a result of that, we need to secure that infrastructure, as the services given to this infrastructure. So, Sri Lanka CERT was established as a result of that initiative in mid-2006. And I have to say that I am one of the founding members of Sri Lanka CERT. And it was formed by the ICT agency of Sri Lanka, which is the apex.

And currently, we are under the Ministry of Telecommunications and Digital Infrastructure. But earlier, when we were set up, it was directly under the Presidential Secretariat. We had authority at that time, but now we have moved to a separate ministry. We are a nonprofit organization fully owned by the government. And the primary function is incident handling. In addition to that, we do consulting services. And our constituency is private sector, public sector, and the general public.

And we are a full member of Asia Pacific CERT, as well as the World forum for Information Security, called FIRST, forum for Information Security and Response Teams. This is my agenda. I will talk about the statistics and the situation of implementation in Sri Lanka. And current cybersecurity situation and legislation, and what are the current collaboration of Sri Lanka CERT, and the future. Some statistics -- more than 100%, most people have more than two -- and these are some of the reported statistics, only reported incident to Sri Lanka CERT.

You may have seen -- you can see that there is an increase in the reported incidents. And most of the them are related to social media-related incidents, but in addition to that, now, from the past few years, we have observed that there is an increase in financial fraud, including ransom and less hacking into email accounts, and some other accounts. And also, it's very common in Sri Lanka. Some

people fly to Sri Lanka to do credit card fraud. In most of the cases, we have found that the people who are captured by police are foreigners.

And we have strong legislation on computer crimes. It's called Computer Crime Act Number 2007, which is also prepared based on the cybercrime convention. And this was brought into fruition in 2008. And the scope of applicability is very good. And it covers broad ranges of offenses. It includes the offenses that use computer as a tool to do cybercrimes, as well as hacking incidents, including wireless. And for the government sector, we have a high-level information security policy, covering around 17 domains.

We added two more, now we have 19 domains. It's used by most of the government organizations. What we do is we customize these domains into the -- we go into the government sector organization and discuss with the people, and the organization, and we customize these domains, the information security domains into the needs of the -- to address the need of the particular organization. And as a result of the -- having this act, we had to set up a separate cybercrime division in the criminal investigation department, and they are the one who deal with most of the cybercrime investigations.

At Sri Lanka CERT, we don't have any authority to do investigations, but we do support the criminal investigation department technically. For the people to resolve the incident technically, but if we found that any reported incident, they need legal support, the criminal investigation department will have a contribution. And regarding the current collaboration, we are a full, active member of AP CERT. And we do activities with AP CERT and FIRST. We contribute to the annual cybersecurity bill, as well as we are in several working groups of the AP CERT.

And in 2011 and 2014, we were the leading team who was organizing the cybersecurity for Asia Pacific countries. We have worked with a lot of CERTs in the Asia Pacific region, as well as other international CERTs in the world, and also worked with cybersecurity organizations and other organizations like Microsoft and some organizations to deal with cybersecurity issues. And I'm proud to say that we are part of the only commission on cybercrime, and we became part of that last year. We are the first country -- member that became part of it.

And these are our collaborations. We are happy to partner with any CERT, as well as if there is any community having -- need to have a collaboration in cybersecurity area, we are very happy to collaborate. And we encourage private to public partnership, because we have found that it is essential to deal with cybersecurity issues. So, thank you very much.

>> BABU RAM ARYAL: Thank you. Just a very quick question. In Sri Lanka, threats are from inside or outside?

>> ROHANA PALIAGURU: Both. Basically, most of the threats are from outside. But inside also, we have found several cases.

>> BABU RAM ARYAL: Thank you. Is Mr. Subhash is online? So I'll move along. After listening all these things, in the bigger economy, it has lots of international companies, they're working in India. And if I remember, in Italy they were reluctant to move their data to India, considering possible very vulnerable data centers in India, and offices as well. So after listening to all these things, what is -- can you summarize the situation of south Asia, as well as the Indian perspective, how we can collaborate on this kind of situation?

>> Sure, thank you. First, on this panel, one of our panelists could not make it, but I think we all come from the cybersecurity perspective from our lens as men. And no conversation on cybersecurity is complete without having communities, especially women on the line. But having said that, on some of the concerns that have been raised, I think India's biggest concern is that -- who things, actually. One is design, and the second is the economy. The design aspect which is common to south Asia -- many countries, I wouldn't generalize, but many countries across south Asia is that we have net information exporters.

We do not retain data, but most of the data of Indian citizens is stored in servers abroad. As a result, we are seeing somewhat -- you know, controversial tendencies of governments in south Asia to localize data, which may not be in the best interest of everybody, but also to see that it goes into communications. And some of it is, you know, driven by legitimate demand to tackle law enforcement concerns that panelists here have told us, you know, the incredible amount of stress that is placed on law enforcement agencies to tackle cybercrime.

But the design aspect, which is that many south Asian economies do not have control over the data -- and I do not mean insidious control, but, share a fact that they are not able to access it for legitimate law enforcement purposes is a problem. The second is the design. One more aspect to the design element which is true for India is that as a supply chain on ICT is entirely driven by foreign suppliers, mostly from American and Chinese manufacturers. This is not a problem in of itself. I think it's a good fact that economies are opening up to good hardware and software products.

But I think it has also reduced the agency of Indian organizations to tackle cybercrime because the supplies -- as a colleague of mine puts it, we are not a dust-based supply chain, but we are a faith-based supply chain, relying on faith in the security of products that are supplied from other parts of the world. On the density part, nearly -- India and south Asia is a growing digital economy if you consider it as a whole. Nearly 72% of Indian firms faced a cyber attack last year.

But the fact is that we -- India -- is adding internet users at a stunning pace. At the end of 2018, India is expected to have roughly 518 million internet users. That is, I think, six times the overall population of France. So it's clearly a huge challenge. And coupled with these design and density issues, what you see is a risk to the bottom. I'm not sure whether that is the case in other south Asian economies as well, but there is this race to the most cost-effective ICT product.

Sometime earlier this year, there was a product advertised which was basically a mobile handheld device available for 251 Indian rupees, four U.S. dollars, less than that. But -- you know, and thousands and hundreds and thousands of Indians enrolled on the website of freedom 251, they realized the information they were providing was not secure. You know, what can you expect of a company that does not control the confidentiality or protect the confidentiality of your information on a website to provide you with a secure mobile phone?

And, you know, this is, again, an unfortunate circumstance by virtue of the fact that many cannot purchase an iPhone. iPhone's market share in the United States is 44%. In India, it is .01%. High-end devices in India don't have that kind of a market. By virtue of having low-end devices, cybersecurity vulnerabilities are also introduced. Last point is also institutional. Many of my colleagues here have mentioned that there are CERTs and computer security incident response teams in their respective countries. That is true for India as well, but there is now talk about having an integrated cyber command.

This would essentially -- you know, it would be an integrated agency involving both the army and the civilian agencies. There are some concerns about what institution would play what role. But I think there is some sort of consensus among the elites that a cyber command would be able to better assess and respond to threats.

>> BABU RAM ARYAL: Thank you, Arun. Recently, I had read a news article -- why we are selling equipment in the Indian market. One promoter is a friend of a Chinese insider, let's say, I don't remember the proper name of the secret service agency. But because of that, there was some issue. Do you think that this kind of thing will hamper the cybersecurity issues?

>> ARUN: I think it's an issue. I don't think any cybersecurity regulator is under the impression that something is entirely free of vulnerabilities. It's difficult to say, if you say the founder is related or close to -- it's very difficult not to find those kind of linkages in China. But you find it in the United States as well. The Department of Defense is coming up with an initiative working closely with Silicon Valley companies. These linkages are unavoidable. What a lot of us have been advocating is to have a common

testing criteria which will essentially involve the major suppliers and vendors of hardware agreeing to a common but rigorous testing criteria for their hardware products, and India, speaking from the national forget, having the indigenous capabilities for testing these products.

>> BABU RAM ARYAL: One more question for you, Arun. We're talking about conversion in south Asian, and we have multilateral comments. I read somewhere in an Indian survey that the impossibility of MLATs is three years. So this is very not much relevant in cybersecurity incidents. So, from that experience, what you may suggest in this area?

>> ARUN: Any attempt to have some sort of a convention, or even there are some political problems in getting some sort of coordinated action in the nations. But even some sort of guidelines between CERTs as well as the cybersecurity -- top cybersecurity coordinators in south Asian would be useful, you are absolutely right. The waiting periods for extracting information through MLATs is just unacceptable. But the problem is also political. You will ultimately need south Asian governments to come together and acknowledge that there are different types of security threats which need to be tackled together.

>> BABU RAM ARYAL: Thank you, Arun. We have been talking a lot. I would like to open the floor. If you have any particular question to particular or in general to the panel. The floor is open.

>> All right. You can use a Linux user group in your country, because you rely on a copy of Windows. I think your country can really use Linux. It helps. It actually has a lot of benefits for people, building of skills, have a functional operating system for people to use. You might not get the best hardware, but Linux is one of those things that you can find. All right. Thanks.

>> Yeah, from Nepal. You know, if you look at cybersecurity, then if you look at the south Asian perspective, most of the countries are very rigid towards open standards. Why is this? All the breaches are happening in southeast Asia, most of them. Are we lacking somewhere? Are we not -- we are not pointing out the exact situation, or thing. We're just talking around it. So, is there any sort of, you know, awareness campaign that is being done in terms of political leadership? Because that's where they do make the policies. That's where they facilitate, right.

So we are lacking in terms of capacity and awareness. That's like hugely in terms of those people, you know. We are discussing here, that's something very credible. We are just talking it here. But when it comes down to them, they are the ones who will be solving the issues. The other ones, it's not like the presentation from a certain department won't count. Because they will be focusing -- if they have the knowledge. So is there any practice, or any campaign,

or any project specifically in southeast Asian countries that is going on?

>> Thank you.

>> I completely agree with you. I don't know about Afghanistan, but to my knowledge, in most south Asian countries, there is a robust open software standards movement. I think there is a tendency we are seeing in many Asian economies to move towards protection, which is a real problem in terms of limiting the ability of entrepreneurs to come up with open standards. I think the move towards intellectual property right regime is coming from outside, mostly through mega-trade agreements, which are one big factor.

I'm not fully qualified to talk about the open software movement, there's a pioneer in this movement. Traditionally, decide been geared towards ensuring that internet access is available for marginalized communities or the differently abled, but now I think especially with regard to security, I think having open standards on software is all the more crucial. I only wish that it was stronger.

>> I think from the Sri Lankan perspective, most of the government agencies doesn't like this area, because of the influence of the organizations in these countries. And people are used to use Microsoft product. They are not open source, but they are user friendly and easy to install, etc. But there are advantages and disadvantages. But there is no strong campaign on open source.

>> AUDIENCE: Thank you. Hi. This is Mohit. First of all, I would like to thank the panel to sharing their thoughts on this important topic and their respective government. But I think the theme of the workshop was the collaboration. And in spite of Babu pushing, asking hard-pressing questions about the collaboration, I have not heard a single instance where the collaboration has happened between south Asian countries. So, I would like to see at least one collaboration effort between the countries. Also, I would like to ask what are these members of these AP CERTs?

I mean, what are the mandate of these AP CERTs, and how are they helping in case of incidents, information flow? This is a knowledge development which happens. We are sharing the common geographies. We are sharing the common threats. So I think it's important that we have that collaboration flowing, and there has to be some organization like AP CERT, or FIRST, or whatever, common ground to have this information flow facilitated.

>> Thank you, Mohit, for these very good questions. In fact, there have actually been attempt within the south Asian region on collaboration in this cybersecurity and related matters. In fact, when this SAARC, South Asian Association for Regional Corporation, this was established back in 1985. The idea behind this was actually that south Asia, almost 1.6 billion, one fifth of the world's population. Because of this significance, it was realized that if these economies collaborate with each other on significant issues

like cybersecurity and stuff like that, only then they can survive and they can evolve, and develop.

So coming specifically to the point that any attempt -- yes. There have been attempts, for example, the convention promotion of convention and promoting welfare of children among the SAARC companies back in 1993, and they have been coming up with conventions -- SAARC convention, suppression of terrorism and related matters. Then there was this meeting that actually discussed telecoms and IT issue, and then the convention, a SAARC convention that actually convened the regional nations and discussed related matters.

But the fact of the matter is not just, you know, sitting together and drafting a document or a white paper. The fact of the matter actually lies in institutionalizing those conventions and those legislations, or memorandum of understandings. So there has been. Implementing those initiatives, but, yes, there have been attempts in the history. And there really needs to be a practical, dynamic approach to institutionalizing these conventions. Thank you.

>> You asked about AP CERT. I will give you some example. Last week. Normally, incidents -- what happen in the AP region. Last week we received an alert from the Taiwan CERT that says that there is something going on and there is a bug in the particular brand ATM machine. And they are recorded that in Taiwan, they have lost -- there are financial reports going on. And as soon as we received that message with the AP CERT mailing list, we disseminated that message to all of the banks in Sri Lanka, so they could take action if they used that particular brand in Sri Lanka.

We knew that brand was used by some of the banks. That is one of the good example, if you need some examples. Previously, there were attacks with the Korean banks. They distributed the attacker's IP addresses to the mailing list for the respective countries, and they collaborated with the Korean CERT in Korea to get rid of this attack. Those are two examples, but there are some other examples as well. But to the AP CERT mailing list, we support each other. And we do a drill so that we will be ready for this kind of incident when it happens.

>> AUDIENCE: For the record, speaking in my personal capacity, I'm from Russia. Across many parts of the world, the cybersecurity card is played quite often to crack down on civil rights and privacy. So my question to you -- because I understand that not only -- you are not only techies, but also civil society representatives, at least some of you -- is there any common ground for the countries of south Asia to collaborate in striking the right balance between, you know, human rights, including privacy, first of all, and those quite understandable public interest in maintaining a high level of cybersecurity? Thank you.

>> PANELIST: Thank you. One of the issues that face many south Asian economies is that the information technology legislation in these countries is invariably drafted in the last decade, in the second half of the last decade. And there was an attempt to foresee developments in technology and try to regulate them by law. This hasn't happened. And now in India, at least -- I can't speak for other economies -- but in India you see a vibrant civil society movement, for instance, towards -- calling for greater encryption, calling out against data localization.

But still as you say, this still doesn't take away from the legitimate concerns of law enforcement agencies. The attempt is to create a multistakeholder dialogue. I'm not sure if it'll go anywhere.

>> BABU RAM ARYAL: Thank you. We are running out of time. Can Mr. Subhash join? Can you move this slide? He has very interesting. For collaboration, next slide. Next slide. Next slide. Okay. Yeah. Thank you. So, he is not able to join because of some technical issues. He is very open with the proposal. And he is proposing subregional CERT or cybersecurity center could be a good initiative. And he also is with initiating cybersecurity toolkits based on similar linguistic and cultural similarities. And another is annual experience sharing program as well.

So these are very interesting recommendations from the government side. And it will be very interesting to adopt the perspective. So, how many times we have? Ten minutes more. Okay. So, can you go up one slide, please? No. I think . . .

>> Hello? Can you hear me?

>> BABU RAM ARYAL: Yes, we can. Subhash, you are welcome. Share your thoughts. We are running out of time. We are almost at the last stage. Can you go through your slides first, and then continue?

>> SUBHASH DHAKAL: Yeah. So I'll continue with my third slide. So, please get me to that. Actually, so, good afternoon, everybody. So, I'm focusing on the regional collaboration on cybersecurity. So because we have some reasons for the collaboration also. Because a part of the south Asian countries, we share the same gateways. So we have the same gateway, Nepal, Bhutan, they use the Mumbai gateway for the connections and everything. And we have initiated a project to connect countries like India, Bhutan, Bangladesh and Nepal. So, this infrastructure and technological connections, but, our society need to use communications with each other.

And our economy -- more or less, if you talk about Nepal and India, we have a broad, open economy. So, for this reason, we need very strong regional collaborations among them. So, next slide. Next slide. Next. Okay. So, as Babu said, we need -- we can have a subregional CERT. So although there some issues in India and Pakistan, I think first place India and Pakistan might have come together when they realized

that we can work together for this. We hope that they will also come together.

So, this is very important, because this country has faced similar problems. If you see the Microsoft reports on the malware situations, we are the five countries from the south Asian region. So we need to focus on that. And we have common institutions which can work on these, because we have established the SAARC universities which can be good institutions conclude focus on this. And my second point is, sharing cybersecurity awareness tool kits based on similarities. This means, if you say Mumbai, they have the same linguistic -- they use the same language and culture.

So cyber awareness tool kits can be used. If you say some -- other countries, they use the same language. Also, we can have collaborations with these -- we can serve those tool kits from one country to another country. Finally, the experience-sharing program, this one is more or less my services that we can instruct. And these activities we can instruct immediately. Thank you. So, I think I could answer one of the questions from the floor, also. That is regarding the open exchange.

So, our government is focusing on the open -- so we don't confuse it with the open sources. So we have already issued the guidance and our agency is already working on using the open (?). And I think that meets with any initiatives, the open government also, because our commissions for right to informations . . . So they are drafting this paper on the open government initiative also. So, that's it from my side right now. Thank you.

>> BABU RAM ARYAL: Any question to Mr. Subhash from audience, please? Thank you. A last wrap-up question, or summary of the conference, can we have -- in the south Asian region? He's listing some using south Asian type of -- one. Another is -- platform to collaborate. He is from government. And he's proposing this. Then I'm confident Nepal government will endorse this. What will be citizen and other countries, if we collectively approach our own countries?

>> Technically it is possible, but practically, given that we have to have a lot of discussions with the governments, it depends on their political views. So to have this kind of collaboration, that commitment from each and every government is essential. We should have a lot of discussions to initiate it.

>> I agree. I think I would be very cautious to say that any collaboration is going to be immediately visible, because CERT -- a lot of organizations that have access to a lot of information. Governments may not be willing to share this information at this stage with their respective counterparts, although it is desirable.

>> Okay.

>> I'm not sure how closely the experts and participants know about SAARC, but there has been an attempt. And they established a university in the area of law, SAARC law, which is a subprogram within SAARC. And they actually established a university in Bangladesh. And, you know, that has been used for capacity building in the area of law. But definitely, there is a potential for a collaboration, corroboration in this area for coming up with something that specifically targets cybersecurity and cyber law, thereby utilizing this platform for capacity building, for communities within the SAARC region. But on the CERT thing, on the regional CERT thing, I very much agree with my friend Arun and Rohana that it would be sort of intricate for the economies within the region to, you know, exchange information and stuff like that. Thank you.

>> PANELIST: I think I agree with Rohana. Theoretically it might be difficult to have a regional collaboration between states. I think it also makes sense to have non-state collaboration between academia. It's pretty practical to go -- you don't have to talk to states to have collaboration. You can have inter-academia or private sector collaborations. And also, it will make a lot more practical sense to have a definite -- or definitions of the information that we exchange. We don't have to exchange, you know, information or data about the incidents, or the scale or the scope of the incidents, but also the best practices, how they approach the incidents, what are the best practices for that, what organizational structures, what procedural tactics did they follow, and what technical skills did they require. I think if we define those, I think even though it sounds theoretical, it will become more practical if we can have those definitions and go beyond states.

>> BABU RAM ARYAL: By the way, do we have any remote participant questions, technical team? I was just missing that part, I'm sorry. Questions from participants? Thank you very much. Thank you all. I am really thankful to all the panelists, remotely participating, Mr. Subhash and Jahangir Hussain as well. And, of course, we'll continue this discussion. We'll have more collaborative -- or practical solutions, not directly -- sensible, but how to elaborate further, how to do these collaboration in south Asia in the future as well. Thank you very much. Have a good day.

(Applause)

(Session concluded at 12:38 p.m.)

***

***