RAW COPY

WSIS FORUM 2022
POPOV ROOM AFTERNOON

MAY 31, 2022

Services Provided By:
Caption First, Inc.
P.O. Box 3066
Monument, CO 80132
+001-719-482-9835
www.captionfirst.com

***

***

>> We will start our next policy session. Thank you. Yes. We're about to start. Yes.

>> AHMAD SHARAFAT: Good afternoon. To those of you who are joining us physically in Geneva. Good morning, good afternoon, good evening to those of you who are joining us across the globe.

Welcome to this session which is Building Confidence and Security in the use of ICTs. In the digital age, trust is everything, cybersecurity is crucial to ensuring universal, trustworthy, equitable access to connectivity.

Today we have imminent speakers and without further ado, I would like to invite first WSIS action line facilitator, Dr. Chaesub Lee, Director of Telecommunication Standardization Bureau, to brief us on the context of the session and to inform how the action lines is being implemented by the respective U.N. agencies.

You have the floor.

>> CHAESUB LEE: Thank you very much, Dr. Ahmad Sharafat.

Excuse me, sir, excuse me, in the middle of this room, we have started our session. Please allow us to keep our sessions going on. This is the session, this security environment is most important for all of us.

Let me start with Excellencies, distinguished colleagued, panelist, thank you. Let us discuss where we stand in our world to build trust in our city.

The pandemic has shown the importance of ICTs and

Digital Transformation to be critical to a sustainable future.

We learned that ICT to important to people's needs and that they are user friendly for everyone, secure and safe. It highlighted access to reliable information, reliable data, nothing less than a measure of safety, in the previous session, it was highlighting that.

We have spent quite long years to address smart risk and we have to continue, it is also time to look at sustainability, how to provide our technology, make societies sustainable.

We have worked quite a lot of years talking about quality, quality of service, experience, quality of life and also we start around the 15 years ago the security measures and the security has become an essential part of our connected lives and also in addition, security, safety, trust, we found that during the pandemic time.

ITU is the lead facilitator of the WSIS action line C5 to build the confidence in the security in the use of ICTs.

Digital Transformation, it is accelerating across every sector of our communities and economies. It was a cybersecurity and trust. I want to highlight the culture of them.

ITU is in a strong position with multistakeholder models.

ITU, global security index, they demonstrate the commitment of ITU members, there are contributions to the cybersecurity.

With that ITU Global Cybersecurity Agenda, we support the countries to define the cybersecurity strategies and we assist the establishment of the response teams and we also support the protection of children online and we assist countries in building cybersecurity skills and also we develop technical standards addressing the security and the trust.

The topics in our study, it is increasing now, like the digital financial services, intelligent transport systems, blockchain, the quantum information technologies. Those are new emerging technologies that are needed with the support of security. Working together in the ITU standard works we're enforcing the new partnerships that will be essential to our achievement of the 2030 Agenda for Sustainable Development.

I believe WSIS process aligns directly with this agenda.

So WSIS action lines are key guiding lights for the digital collaboration required to achieve the Sustainable Development course.

The questions raised by the pandemic asking us how we plan to live together, harmoniously as an interconnected global society, so we are deeply invested in this debate. I look forward to our continuing to work together to ensure that our many interconnections help us to care for each other and to build a better life for all.

Thank you very much.

>> AHMAD SHARAFAT: Thank you very much, Mr. Director, for your comments and your information.

Without further ado, I would like to go to our second panelist, we have professor Philemon Zoo Zame from Cameroon, Director General of the agency for regulation of telecommunications.

I have two question, sir, for you, how does the resilience of ICT infrastructure manifest itself in Cameroon, and what would be the coulden create usefulness for a country like Cameroon which has made significant progress of the possible establishment of a Global Fund for the development of ICTs? You have the floor, sir.

The presentation can be English or French. We have live interpretation, feel free to speak in French, if you wish. Thank you.

>> PHILEMON ZOO ZAME: Thank you for giving me the floor. Thank you for inviting us to participate in this WSIS Forum.

Thank you to our government's action Cameroon has progressed quite significantly and it is quite well off in terms of resilience of ICT infrastructure because it has electronic communications transport operator offering other concession holding and network operators.

The national, international transmission capacity services such as urban and interurban transmission services via fiberoptic, microwave, satellite links, VSTAT, international transmission services through four submarine fiberoptic telecommunication telecommunication cables and a satellite tell port and Internet connectivity. We have a national transmission network covering the entire country as well as the capacity to establish direct international access.

Furthermore, Cameroon is currently finalizing the rollout of the national emergency telecommunications network which is specifically dedicated to cost of emergency services which may be used by populations all around the country.

Also, a regulatory authorities for telecommunication secretary in Cameroon has acquired and put in service an emergency electronic communication platform two years ago. In the event of a disaster that would totally or partially effect the operation of the network open to the public the system will enable the network to be resilient.

We're working together with other government structures to protect our cyberspace.

Given all of the above, to answer our second concern, despite recent progress made in terms of telecommunication, ICT infrastructure in Cameroon, especially the fiberoptic rollout, Cameroon, just like many other African countries, it is still -- it still has to contend with many issues related to education, agriculture, food, public health, basic infrastructure or even defense and national security. This leads to the fact that available resources are focused

towards priority areas, despite the lack of resource to allow for universal access, the government does work to increase access to broadband in rural areas, on each agenda specialry fixed broadband in urban areas. The penetration rate of fixed broadband telephony remains low, Cameroon remains the country that is nonetheless most connected in our area. Given the current global economy, meetings between economic stakeholders from the five continents essentially occurs through electronic means and we're therefore continuing to develop the infrastructure as well as our regulations in order to appeal to the strategic investors or to increase supply and demand for equipment and services.

This is the figures of our head of state in Cameroon so that Cameroon may participate fully in the digital revolution.

We therefore suggest the possibility of setting up a Global Fund for the development of ICTs under the Egis of the U.N. and the funding of this fund whose action would complement the action carried out by specialized institutions such as the ITU could involve multiparty entities, the COVID-19 pandemic has taught us that in this digital revolution no country, no area should be left behind which justifies this Global Fund.

Such a fund will help developing countries which have a huge potential of economically and socially to upgrade the performance in terms of access to ICTs wellbeing and inclusion of their populations on the one hand and to contribute effectively to the development of the world economy on the other hand.

Thank you very much for your attention.

>> AHMAD SHARAFAT: Thank you very much, professor, for your remarks and comments.

Next I would like go to our next speaker who is remote, Madam Secretary of State, Secretariat of government and Digital Transformation at Presidency of the Council of Ministers in Peru, I hope that we have you online, Madam Secretary.

>> MARUSHKA CHOCOBAR: Yes. I'm here. Hello.

>> AHMAD SHARAFAT: Thank you. Thank you very much. Good to have you with us.

I have two questions, first, how can we provide public awareness on responsible use of digital technologies and what is the value of your country's interaction with international organizations on this issue? That was the first question.

The second question, what is the representation of women in digital security, and how have you encouraged more women to embrace their responsibilities on cybersecurity? You have the floor, Madam.

>> MARUSHKA CHOCOBAR: First of all, I would like to say thank you to the ITU for the opportunity to present the programme perspective on these very relevant matters in an increasingly Digital World. In this sense, I would like to

comment that when we talk about the awareness in the population we need to focus on the cultural diversity, geographical situations and other conditions that exist in our territories. Peru is a country with more than 35 million people, a huge challenge in connectivity and more than 20 million citizens and we have a great opportunity with mobile connectivity, more than 9% of the citizens use cellphones to access the Internet. Peru has been growing in the international indicators in the last three years, and we scale up in the eGovernment digitalization indicatorers ITU cybersecurity and global tech index. In Peru, we have digital governance in the country and in this context, the Internet has emerged as an important pillar for information, communications, interactions related to our daily lives.

In that sense, a new stat has emerged where it is promoting cyber wellness in society. This is for awareness on how to be safe appropriately and to protect ourselves -- one's self.

In other works, now more than ever, it is important to acknowledge the skills and motivation to use the Internet in a safe, responsible, effective matter in a society.

The digital citizen that will be executed in a responsible way n means behaving locally, protecting privacy and that of others, recognizing your right and responsibility when using the digital media and thinking about how your online activities effect yourself, other people that you know, and the online community. There is a public awareness of the responsibility of using digital technology, again rating the developing literacy skills, it is essential for promoting cyber wellbeing. That's why the national platform and alliance for a safety Internet were launched in Peru as a result of the public private joint initiative. The format is a market base of the digital skills development and the leader involving in the publication of the guidance and the knowledge content about the risk of their Internet and the measure that one can leverage all of the benefits of technologies and we're currently in the design of the digital rights framework which we continue to have the incorporation of the Digital Rights Foundation and tools into our local strategy and policy.

On the other hand, the interaction with the international organization is critical to exchange best practices, early awareness of cyber threats and mitigates the threats such as cybercrimes, cyberattacks on a critical infrastructure among others.

On the other side, the gender gap is increasingly visiblable in the technology disciplines around the world. In the latest report, the world leading cybersecurity professional organization found that the percentage of women in cybersecurity is only 24. There are certain reasons why women do not choose to pursue a career in cybersecurity, the reality, it is a notion that it is tasked for everybody.

From our perspective, a way to attract more females to the digital security ecosystem is to provide infrastructure and mentoring which should be done from the early age such as school level.

In Peru, our efforts, our concept in capacity building, we have started by developing coding book notice Peruvian regions from 8 to 12 years and the cybersecurity and national centre developed a number of free online courses that are available in the digital talent national platform.

I'm very proud to say that in our national digital security standard, 80% of professionals are women.

We believe in the impact of the the Digital Transformation in our lives and we will continue working for a digital -- for a digital Peru.

Thank you very much.

>> AHMAD SHARAFAT: Thank you. Congratulations on the remarkable achievements in your country, the beautiful country of Peru.

Next we're going to our next panelist, Dr. Felipe Alfonso Hernandez Maya, the general coordinator of user policy, federal telecommunications Institute of Mexico. Sir, I have two questions to you.

First, what do you consider to be the main issues that governments should work on in terms of cybersecurity and second, what actions are being implemented by your organization, by the IFT of Mexico in terms of cybersecurity? You have the floor, sir.

>> FELIPE ALFONSO HERNANDEZ MAYA: Thank you, Ahmad Sharafat. Thank you to the ITU for this important invitation and discussion of such a great topic as Dr. Lee reminded us.

As we all know, the daily use of communications and ICT services, it has brought benefits to the world. However, it is unreliable that the risk as has been said with the use of the technologies are increasing and in this respect let me show you or try to explain to you what is going on in Mexico.

For example, in 2020 the 26% of adelecents aged between 12 and 19 experienced some form of cyberbullying with females being the most exposed by reaching 29%, many have been victims of identity theft and received messages and others were done with people with false identities. However, only 27% of parents in Mexico monitor what children do on social network, 66% do not use parental controls, and 40% do not know if a stranger has tried to contact their children under their care. Mexico is the third latin American country with the highest number of cyberattacks on businesses, reporting 1.7 million, regarding the economic costs of such attacks it is estimated that worldwide they reach 6 trillion-dollars.

With respect to the banking service, more than 62,000 complaints received for possible fraud of which 35% were for unrecognized consumption, followed by unrecognized bank transfers with 24% unrecognized charges in the deposited account with 14%.

Given these events and figure, which we believe are replicated in most countries, we consider that the main issues on which governments should focus are relation, collaboration, widespread of information. Regarding the first, it is necessary to have standards with provisions and protocols and punish all types of cyberattacks and infringement of rights in the digital environment.

Regarding collaboration, it is necessary to generate synergies between the different government agencies in charge of digital security in the countries to ensure coordinated action.

As well as with other stakeholders, companies, academia, technology generators, in order to implement the existing relations and develop and promote cybersecurity projects.

We consider that regarding the promotion of confidence in the digital ecosystem this is of most importance of the IFT in Mexico and it is a priority line of action to be implemented in the medium term. We believe it is important to develop information programmes and campaigns to promote digital literacy and encourage informed and responsible use of the Internet.

Let me explain to you, to the floor, Mr. Ahmad Sharafat, what actions, as you have been asked what are being implemented by the IFT in Mexico in these terms. We have taken an active role in this area and has undertaken several lines of action in promoting a reliable digital environment.

We have issued a series of provisions that allow from attributions to contribute to warranty, security, trust, info vagues for the development of the digital ecosystem and we collaborate on an ongoing basis with other government institutions and academia to organize workshops and Forums to generate and provide updated relevant information on digital security.

In the area of providing information, since our creation, we have been designing various informative materials about cybersecurity such as guides, capsules, infographics, among others.

We have created a way to display materials such as capsule, infographics, graphic, steps, other, and this information is available in five different sections. For children, parents, small, medium enterprises and other sections about general recommendations.

For the development of the programme, collaboration is held with different entity, including the government agencies, civil associations, private initiatives relevant to the promotion of the digital literacy and the promotion of informed and responsible use of the Internet users in Mexico.

My time is finished, and these are the main important things and how it could be useful for other countries.

Thank you very much.

>> AHMAD SHARAFAT: Thank you very much, Mr. Felipe Alfonso Hernandez Maya. Congratulations for your

achievements and for your remarks and way forward that you proposed in facing difficult issues on cybersecurity.

Thank you very much.

Next, we go to our next panelist, Ms. Afke Schaart, senior Vice President of global government affairs department in Huawei technologies in China. Welcome to our panel.

Two questions, first, in the digital era, cybersecurity resilience based on anti attack capabilities and swift recovery plays an important role in the construction of the infrastructure to ensure cybersecurity and provide more secure, reliable information services for society.

What roles and responsibilities should different stakeholders play in building cybersecurity.

Second question is, in the telecommunication field, what roles should stake players have for enhancing the 5G cybersecurity management across regions, country, sectors, and what measures, baselines, practices, can be shared in terms of government regulations and technology and standards.

Madam, you have the floor.

>> AFKE SCHAART: Thank you to the ITU for having me here today.

I would like to congratulate you with another successful event and bringing us together to to discuss the future of telecommunications. My name is Afke Schaart and I work for Huawei and I'm base where had the company was founded 35 years ago by our CEO and I think that most people know Huawei but I want to stress we're a leading global ICT infrastructure company and smart devices and we have 200,000 people working for us all over the world and half of them are in R & D. We operate in 170 country as and regions and we serve proposal 3 billion people around the world. Security has always been at the core of our business because we exist to serve our customers and are committed to the secure operations of our customer networks and services and for the panelists today, I would like to make four points if you would allow me.

So, first of all, cybersecurity threats should be fact based and based on experience. The reality is that cybersecurity threats are everywhere, they're increasing, no one is immune. It is important that these threats analyzed are based on facts and experiences so that stakeholders can build resilience models and discuss solutions from Big Data, analyst and fact-based experiences is the first point.

Secondly, we need to develop resilient solutions based on standards and rules.

What the ITU is based on.

So the communications industry is a highly standardized industry, one of the best examples on how a sector can work together to come to global standards and I think that's due to the excellent leadership of the ITU and the technological evolution that we have seen from going from 2G to 3G and then now 4G to 5G, it is going to be driven by standards and

specifications.

Existing gaps, they are still there and cyber resilience indicates that the global standards products are still not optimal and some regulations are not being regularly enforced.

For example, a main cause of data leak, fortunately both products vulnerabilities and the operational lapses can be addressed in well established standards and regulations, and I'll give you two examples.

First of all, the framework that's jointly released is a good example on how to address the issue.

It draws upon industry experience and provides a clear clarification framework for product security assessments. In addition, there is a 5G cybersecurity knowledge base published with input from global operators and suppliers. This provides guidance on how to systematically address the 5G security risks in different stages from network planning, construction to maintenance, optimization and operations. These fact-based approaches are widely supported by players across the industry and we believe that governments and regulators should also consider adopting and promoting them as factual standards.

Private firms, governments, they lack the expertise that only industry associations and standard organization cans provide.

We should include them in our multistakeholder framework as powerful source of expertise.

So, my third point, it is that every stakeholder has it own role to play and its own priorities and responsibilities.

Governments have every reason to strengthen industry regulations to serve the public interest. However, overregulation could lead to higher OpEx for the private sector, reduce competitiveness and operational difficulties for operators to in turn undermine the interests of consumers.

That is me coming to my last point.

It is also already said by the lady from Peru and it is very important to stress, we need to attract more women to work in our industry. Motivating women to work in technology innovation remain as challenge if you consider the estimate that by 205075% of the jobs will be related to STEM and we need to develop ICT skills that are more diverse than ever.

Thank you.

>> AHMAD SHARAFAT: Thank you very much.

Thank you very much, Madam, for presenting the views of the private industry in our session. Thank you very much.

Next we go to Mr. Rashid Ismailov, President of VimpelCom, the Russian Federation, I hope that we have you online Mr. Rashid Ismailov.

I have a question for you, Mr. Rashid Ismailov. Welcome to our meeting. The question is from the perspective of Telecom carrier, could you elaborate on the importance of

security and trust in infrastructure, platforms, services? You have the floor, Mr. Rashid Ismailov.

>> (Poor audio quality).

-- 40 million subscribers, I must confirm that the cyberattack on the civilian infrastructure of the Telecom operators have intensified many times over the last years. This is aggravated by the fact that these are not simple attacks any more, they're like, you know, attacks dealing with cryptography and they're hitting the infrastructure itself. Creating the main problem, credibility in technology and trust in technology.

The intention with the 4G for example, we have recently the statement of a President who said that by 2030 that smartphones will be replaced by variable electronic products and even implanted chips in human bodies, it seems to be vague if we will not solve the problem with the cybersecurity. The developed technology right now, I mean, after 4G, 5G, we witness and see the growing of IoT, Internet of Things, telemedicine, so far, so forth.

Unmanned vehicles.

Previously with thinking about the threats as it works with the personal data, that's about GDPR and other fundamental laws that have been adopted in Europe for example.

Now with talking about the mere existence of the -- (poor audio quality).

-- the risk, it is that simply without solving, as I said, the problem with the cybersecurity, not able to, you know, go forward.

(Poor audio quality).

we have a handful of countries that really from the technology point of view, you know, sustained their sovereignty, meanwhile, others, they would like to be -- to keep this because they face a lot of transborder kind of information flow, attack so, forth, so on.

However, the availability of the Internet, it is -- it is the bumps actually, it is the border, there are no borders, and this, you know, this dilemma we have to solve, as a society.

For Internet sovereignty, due to its nature, the global technology structure and structure of governments, the Internet does not provide this with the cross-border exchanges. The infrastructure, especially global infrastructure almost inevitably is a fact of -- (poor audio quality).

As I said for the vast majority of countries, the sovereignty does not allow them to claim a independent role in the global information space. Today ICTs have the same decisive impact on the national global development and they also data mine the degree of sovereignty like nuclear technologies in the 40s or the last century with the space technologies in the 70s or the 20th Century.

Infrastructure sovereignty, it is first of all the ability of the network to operate even in the event of catastrophic shut down of the main cross-border channel. This is not isolation from the global network, this is insurance the problems.

States in this case must act from the considerations of preserving their own sovereignty and from the understanding of the global nature of the Internet and the Information Society.

In the absence of the effective international law in the field of the Internet it turns into a space (poor audio quality).

Cyber warfare without rules.

Users benefit from the Digital World if country also support the fifth law of information while respecting applicable domestic and international legal framework and I must say that if you take Africa for example, a month ago, the first cybersecurity Forum Congress in total, among the tools put forward to strengthen cybersecurity in Africa, the declaration, it is a policy document that convenes the establishment of a specific legal and (poor audio quality).

>> AHMAD SHARAFAT: We are a bit behind schedule, I would like to ask you to --

>> RASHID ISMAILOV: I must say, from the business point of view, cybersecurity requires huge investment and recently in GSMA for example, there are lots of discussions, the biggest content providers should, you know, invest into the infrastructure and that's supported and we think that it has to be shared. The investments in the network and the investments in the cybersecurity as well. Thank you.

>> AHMAD SHARAFAT: Thank you very much for your remarks, for the comments that we do appreciate.

We wish you all the best.

We now go to our next speaker, Mr. Mohamed Ben Amor, Secretary-General of the Arab ICT organization in Tunisia. Welcome, Mr. Mohamed Ben Amor.

I have two questions for you.

First, COVID-19 pandemic has accelerated the Digital Transformation across the world. What is your vision on gaining the users' trust and what role AICTO, your organization, is playing at this level in the Arab region.

The next question, the last layer, Arab ICTO, they have developed the vision of cybersecurity, could you give us a description of the strategy, its goals, outputs and to what extent do you think will enhance the cybersecurity readiness and response to cyber threats within the Arab countries? The floor is your, please.

>> MOHAMED BEN AMOR:

Thank you, Ahmad Sharafat, for the two important questions.

Let me begin by thanking and commending the ITU for an excellently organized WSIS Forum which has made it possible

to put information and communication technologies at the top of the country's listed priorities. We are reminding ourselves through the Forum of the importance of technology to give better lives to our citizens throughout the world.

I come back to your questions now. As the other speakers have mentioned, especially Dr. Le e, the public crisis confirmed the importance of digitalization and was a springboard for Digital Transformation at global level since the beginning of 2020.

As players in the IC T Sector, we are working for Digital Transformation and for it to be trustworthy, worthy of trust.

We're aware of the crucial importance of digital confidence in the Digital Transformation process in the Arab world and our organization, we have launched several initiatives and projects. We have the regional digital trust network, it is an interregional, multistakeholder network for digital trust in the African and Arab region. It is open to all stakeholders, and the key aims, it is convergence, harmonization of the regulatory, legal frameworks, secondly, mutual recognition of digital trust services, harmonization and development of standards on digital trust.

So far, we have 15 countries represented by their certification authority -- electronic certification authorities in the Arab and African regions. African and Arab countries, as we work on digital trust, we launched a survey at the beginning of the year for information on the State of play and achievements in this area. The results of this survey, it will be used as a key tool to establish a common framework for digital trustworthy services.

Digital trust and competence in cybersecurity are top priorities that require sound, cooperation, relationships, at international, regional level so that we can have a cooperative approach with the trust of all stakeholders.

In this framework, we count on the international, regional cooperation with several agreements with the International Telecommunication Union that Standardization Bureau represented here by Dr. Lee, the Asia PTI, on the framework of tried actions. With respect to the second question that I mentioned earlier, cybersecurity is a key topic in our region and we have the Summit, the international, social Summit where we worked on the vision for cybersecurity that was launched in 2021 in the presence of His Excellency, the President of the Arab States. Thank you for your attention. I hand the floor back to you.

>> AHMAD SHARAFAT: Thank you very much, Mr. Secretary-General for the comments. Congratulations for the excellent work done in your organization.

Our final panelist today, it is Mr. Nazarius Kirama, President and CEO of ISOC in Tanzania.

I hope that we have you, sir, with us online. I have two questions for you.

First, as a Civil Society stakeholder in Kenya, you're involved in confidence and trust in the use of ICTs for end users, how are you doing this? That's the first question.

Second question, it is that on the training and awareness to build confidence and trust, what specific groups are you engaging in Tanzania in these areas? Sir, you have the floor.

>> NAZARIUS KIRAMA: Thank you, professor. Thank you to everybody in the room. I'm glad to be the last of the ITU this year for the WSIS Forum 2022.

First of all, I would like to thank ITU for, you know, accepting our presentation and for taking me to be one of the panelist this year.

Basically, I will try to combine the questions. What are we doing in Tanzania, like, you can see on my background, you can see the women and youth digital innovation hub project.

Our journey to build what we're doing in Tanzania to build capacity for youth and women, really emanates from the goal number 4, quality education in the target number 6 on literacy and fumecy. And what we have done basically is to expand a little to include digital literacy as part of the package because we believe in what we call in Tanzania, the mass digital literacy for the digital economy.

What we're doing it is to ensure that we build the local capacity for the young men and women and create innovation hubs that can congregate young people and boys and girls to be able to learn the basic skills of digital life.

With that, that will help them be able to actually build the confidence to be able to take on the digital economy of the future.

We believe that investing in universal digital skills and education to target young men and women and because the users and the serious contenders build the blocks of the future, the global digital group and we're engaging women and youth to learn the basic essential skills in the digital goals and security so that they can themselves build trust to use the Internet, to use the devices and to use the digital spaces to innovate and to create and cocreate and also to be able to monetize the content that they have created with the confidence.

With that also we're providing an Internet access to the young people and the communities through the commitment arrangement so that we can take that further.

In the next century we believe that nations that invest heavily in mass digital literacy or universal digital skills education will be able to reap not only the confidence and the security in the use of ICT but also create transformative and competitive citizenry who will confidently take on the future global regional and national digital economies and enjoy the variety of benefits that come with it.

That's why we believe that what we're doing we're

actually connecting young men and women and general public in Tanzania to the digital opportunities and through that, through the capacity that we're building locally, actually they are giving them confidence and the security to be able to continuousing the digital goods for them and for the community.

Lastly, I believe despite investing in infrastructure and all these high end equipment and applications, it is important, and it is a call for the measures of the world to be able to invest heavily in the mass digital skills education because investing in education they will be able to build the security as well as the confidence for the end users who are actually important in the whole equation of cybersecurity ecosystem.

With that, I thank you very much. I thank you for the opportunity to be able to be part of the WSIS 2022 Forum.

Thank you very much.

>> AHMAD SHARAFAT: Thank you very much, Mr. Nazarius Kirama.

Thank you for your remarks, also congratulations on the excellent work that you're doing in Tanzania.

We have come to the end of our session. Let me first thank our panelists for the contributions, whether physical or virtual. Thank you very much.

Also I would like to extend a very warm gratitude and thank you to all of you that have been with us and participated in our meeting.

A final summary of this session, it will be provided tomorrow during the closing of the high-level policy session, which will take place from 17 to 18 hours in this same room as I said, tomorrow.

With this, again, I thank you very much for your presence and this session is now closed.

Thank you.