RAW FILE
ITU
WSIS Forum 2023

High-Level Policy Session 3: Building confidence and security in the use of ICTs
Room D.
https://www.itu.int/net4/wsis/forum/2023/Agenda/Session/139

***

***

MODERATOR: Can I ask if everyone can be seated quickly. We need to start to stay on our schedule.

I would like to welcome everyone, Session 139, Session 3 on your Schedule to this shan important topic as we move further into the digital world and security, trust, and infrastructure are critical for moving us forward and actually addressing this WSIS Action Line and actually enabling numerous Sustainable Development Goals.

So with that note, I would like to turn it over to our WSIS Action Line Facilitator, you can have the mic. -- that we see from large language models and Web 3.2-related services, the Metaverse is also bringing in new opportunities, and also new challenges. At the ITU we started a new focus group on Metaverse which we're looking at these areas and last week the group met to talk about exactly these issues, you know, and having said all of this, our laser focus is on capacity building, you know, on helping countries establish national SIRTs, helping countries get their cybersecurity strategy in order, you know, connect CyberDrills for coordination purposes, you know, there are so many areas that we are focusing on and the bottom line is that we're doing it all in, you know, in a multistake hoilder way with multistakeholder partnerships because we realize that was the way to go and hope that's the key message that come out of this conversation.

>> KAREN MULBERRY: On to panelists. I have two questions that I will ask you, I will ask both at the same time so you can address them within your four minutes. To get started, I have

Mr., Honorable Mr. Ousman Bah from the Republic of Gambia., you're invited to share strategies and highlighting success stories in implementing digital resilience and proposed ways to accelerate the implementation of the WSIS Action Lines digital cooperation, and Ministers are invited to share their views on the WSIS + 20 review and Beyond 2025, and to take stock of the achievements and key trends, challenges, and opportunities since the Geneva Action Plan.

>> OUSMAN BAH: First and foremostant Gambia Government I wish ITU congratulations. It is a pleasure highlighting challenges and success stories in implementing digital resilience as well as our view on the WSIS + 20 review.

Excellencies, distinguished ladies and gentlemen, creating the ministry of education digital economy in May 2022, reinforced the Gambia Government recognizing a commitment to ensuring the optimal utilization of ICT for social demonstration. Also desired great the achievement of UN and Sustainable Development Goals in the Gambia, and through the ICT development -- through the ICT 4D policy 2018-2028 the Gambia government taken significant strides to ensure inclusiveness in use of ICT in the 8th strategic pillar, focus on leveraging the ICT and enhance outcome across all walks of life.

These also include empowering women and girls and vulnerable groups through the use of ICT. The Gambia utilizing climate smart technology and health, starting the mitigation and strategy, which includes the deployment of ICT anchored ally and warning system that have helped in the better preparedness and more informed response to climate change.

Government has also put in place a strategy to control e-waste and also climate on friendly practice from the ICT sector. The Gambia is also stepping up effort and promote social content development in ICT through utilization or through prioritization and optimization in talent in the ICT sector. In rollout across the country, it will help increase the preparation of the locally-developed ICT solution, and also importantly create an avenue for the development of solutions that present the Gambia in a social culture identity.

Also striving to cyber resilience and information systems and processes through implementation of sounds security policy as well as regulation. Excellencies, distinguished ladies and gentlemen, on the WSIS + 20 review challenges and opportunities, it is imperative and to acknowledge the evidence of the digital divide as one-third of the world population is still not connected. We have to find ways in connecting the excluded throughout the means of universal broadband and provisioning of last-mile Internet connectivity in the resilient and affordable manner.

In the same challenges, connectivity accessibility -- affordability and low digital literacy affected my country, the Gambia with imminent implementation of universal access service, US -- UAS policy. The government is committed to ensuring the last-mile access to ICT in Gambia and imam proving broadband connectivity beyond 50% as 2021. Chairman in conclusion, my delegation would like to call all stakeholders to look into measures that can reduce the cost of services and devices and network to support or utilize our digitalization process and connect the unconnected 2.7 billion people around the globe.

Finally, I wish to seize this opportunity to express on behalf of the Government of Gambia the renewed commitment of support and collaboration in achieving the WSIS Agenda, and we believe that innovation and capacity development and interoperability of systems are a cornerstone of the ICT becoming a Sustainable Development Agenda. I want to thank you all for your kind listening. Thank you.

>> KAREN MULBERRY: Thank you very much. Next is the Minister from Nigeria who sends apologies and sent a replacement. So please, two questions that you are to answer. The COVID-19 pandemic shows the great importance of Cyberspace with the growing number of cyber threats also that showed that there was still a great need for cybersecurity awareness in order to ensure that users of digital platforms are not at the mercy of cyber criminals. What have you done in Nigeria to increase the level of cybersecurity across the country?

And, in your book, cybersecurity initiatives for securing a country, you outlined how government plays a significant role in developing policies, establishing institutions, and building the relevant infrastructure to enhance cyber resilience. Can you let the WSIS Community know some of these initiatives that have been successful in Nigeria? Thank you.

>> Nigeria: Thank you very much. Like you said, I bring warm greetings from the Honorable Minister of Communications and Digital Economy. He was here in the morning, but had to leave for another assignment. He sends his regrets. I would like to thank the leadership of the ITU for this opportunity.

Straight to the questions. I mean, it's obvious to everyone that digital platforms became a necessity as a result of COVID. Many institutions, sectors that otherwise will have just done things physically had to, are compelled to move to online platforms. In fact, there is a joke that says that what's led to digital transformation in many countries, it was in the policies of the institutions, but it was as a result of COVID. So many people went to online platforms and that also happened in Nigeria. The flip side was that as a result of

people going to online platforms without being adequately prepared, it opened the door for many people to face the attacks of cyber criminals, and in Nigeria, what we did was that we had to start an aggressive campaign. I like what Mr. Preetam said, he said a laser focus on capacity building, that's what ITU has been doing, in terms of cybersecurity. So in Nigeria, we focused on that. We have a national digital economy policy and strategy that is made up of a number of pillars. One of those pillars is dedicated to the issue of cybersecurity, and it is the pillar called the Soft Infrastructure Pillar, so it focuses on things like cybersecurity, focuses on things like digital identity, focuses on data protection and privacy.

Now, it's impossible for you to really be able to secure cyber specifically if you identify people, and that's why the Minister has given a lot of attention to the issue of national identity, and in fact prior to the time that the national identity management commission was transferred to his supervision, we had just barely 39-million records. But within less than two years and these records were over a period of 14 years and in less than 2 years, those records went from 39 million to over 09 million and shows that replaced on digital identity and others helped us a lot.

We've also done something called name sim linkage because we realize that most people have mobile devices, but if it's not tied and properly identified, then those could be avenues for cyber threats and cybercrimes and things like that.

And so we've prioritized that with doing things in relation to data protection, data privacy, we've ensured that our citizens in the country have access to digital skills online, as there was a national broadband plan launched by Mr. President, and after that launch, he also launched a digital skills training. Unfortunately, it just coincided with the lockdown, and we thought that instead of just getting the people to sit down and not do anything, we had these digital skills online. We collaborated with companies like Microsoft to train 5-million people. That way we were able to get people to understand what cybersecurity is, and to help them to protect themselves online.

You know, initially people used to focus more on cybercrime, but the Minister had -- has started this campaign where he has emphasized the fact that cybersecurity is actually more important, so it's more important to prevent the crime than to try to fight the crime. In fact, the national assembly, we had some committees that were called, committees on ICT and cybercrime, where because of this publicity it's changed to ICT and cybersecurity, and so these are some of the things that have been done. We have SIRTS that have been created, we have issue

of PKI, public infrastructure to strengthen security in the country. Thank you.

>> KAREN MULBERRY: Next we have honorable Chaiwut. Minister of digital economy in Thailand. Here are the questions. What are Thailand's policies on building confidence and security in the use of ICTs? And what are Thailand's success stories and best practices on fighting against cybercrime? Thank you.

>> CHAIWUT THANAKAMANUSORN: On behalf of the government it is a great honor for me to be part of this session on the WSIS Forum here in Geneva. The Thailand government has been promoting investment in ICT and digital infrastructure. This supposedly has been quite effective, and digital infrastructures have rapidly improved. And our infrastructure is among the best in the world. Thailand 5G has covered over 58% of nationwide and 100% of city in Thailand. To make the most digital infrastructure, we have put great deal of effort to build a confident and security in the use of ICT. In particular, we have cybersecurity Law and also established national cybersecurity agency as a possible body.

Not only the cybersecurity law, but we also have past-related digital law, such as personal data protection, and also established organization to listen for this, and we have what they call digital ID to identify the people using online activity.

And also, cybercrime and others have occurred across the world, including Thailand. To fight against online scams, the Government has just approved a new law that -- measure to cybercrime prevention and separation. Firstly, the laws allows financial institutions to peedly suspend suspicious transactions in bank accounts, and the new laws implicitly state that anybody who will allow other people to use their bank accounts or mobile numbers for illegal activities will be fined for three years. Under the new law, mobile numbers and SIM are required to be registered in order to prevent any illegal activities.

Secondly, the laws aim to utilize AI and digital technologies. This is to facilitate financial institutions, telecom operators, and related authorities to timely identified suspicious transactions, such as illegal financial activities, which are some underlying business and able to promptly suspend those transactions.

The law has more effective collaboration among financial institutions, Internet and mobile operators, finance and telecom regulators, and law enforcement and relevant agencies. The new platform will allow data exchange and verification of relevant information among related parties. We believe that the new law will be able to prevent online scams by taking evidence of

technologies and to improve inter-agency collaborations.

KAREN: Next Minister of communication and technologies from Tunisia, Dr. Neji. What are the measures taken by the Nunisia government to protect the national Cyberspace, and what are the main pillars of the Tunisia cybersecurity strategy?

>> NIZAR BEN NEJI: Thank you for the question. I will speak in French and give a brief introduction about the legal institution and technical framework leading with cybersecurity and cyber community in Tunisia. I will switch. I'm sorry.

In Tunisia, we already started to implement a legal framework that has cybersecurity. Last year we completed our texts with a framework on cybersecurity in order to protect from cybercrime that were not sanctioned by the legislation at the time and is also going to regulate investigations, proof analysis, and everything that relates to inquisitions in the area.

A few days ago we updated the cybersecurity legal framework. We had a framework that dated back to 2004 that was no longer adapted to the current cybersecurity issues, so in a few days the new text was published, and this new text including several points and covers a number of important points, so regulating cybersecurity, the mobilization of Cloud service providers, and everything that has to do with hosting, national Cloud, and organizing all the activities. The new text also introduces the new solutions for equipment and solutions at the national level in order to collaborate with the creators and collaborators in this framework in order to provide the solutions, the high-level solutions and ensure that all the users have access to solutions.

We have also regulated everything that relates to the SIRT with computer mernl see response teams that can intervene in case of incidents for maintenance purposes to avoid loss following attacks, cyberattacks or other issues. We also introduced a pioneering measure, a classification notion in order to classify the businesses, according to a certain list of criteria, and it will be published on a yearly basis in order to encourage companies to proceed to audits according to the different host providers and use of tools and recognized and recorded solutions. This is going to encourage companies to implement all that is required in terms of cybersecurity. That is the legal framework. We also have an institutional framework with three agencies that are responsible for cybersecurity, and the knacker nal agency for cybersecurity, the national agency for trust, reliability, and all that relates to proof of identity, et cetera, and finally we have the agency that is responsible for investigations and legal aspects. Thank you.

>> KAREN MULBERY: Thank you very much. Our next

panelist is Dr. Mohammed Al Kuwaiti, head of cybersecurity for the UAE Government. Your question, sir. The UAE cyber model, what does it, has it, what does it do? The unique features? How is the UAE cybersecurity council working to foster innovation growth in the cybersecurity industry within the country? What role does that council play in regulating and overseeing critical infrastructure and security in the UAE? And how does the UAE cybersecurity council collaborate with other countries and international organizations to combat cybercrime?

>> Dr. AL KUAITI: Thank you to ITU for bringing us together with all the distinguished guests that are really providing great models that we learn from. UAE, definitely going through a great digital transformations. We heard today as well from our Director-General on the TDRA and how all of this digital transformation is actually impacting not only one single sector, but across so many actors. And not only that, but as trying to export this model to other nations, as we did in Expo2020 where we hosted more than 193 countries, as a matter of fact, and provided with a great opportunity of learning from the UAE model in that perspective.

There are three maginger important things that we actually will say distinguish the UAE cyber in comparison with many of those things. One is the ecosystem. The ecosystem that we have, it's not only the governing, the policies, the technologies, and the people behind that, but it's also all of the personnel, private sector as well as government sector who works together in order to make this a reality. And this ecosystem really sets a great opportunity of innovating as well as creating many of those ideas.

UAE cybersecurity strategy, for example, focusing on five main pillars, governance as well as protecting and defending in order to really build that resiliency, and as well in partnering with many of the entities, and one of the major pillars there is to innovate. Innovation is what distinguishes us, again, in many of those aspects, and having all of the small and medium businesses helping us together in bringing the reality of what this technology brings to humanity, and that's where we actually go with many of the technology and really is that technology to be leveraged by many of the entities. And one of the other major distinguishing things that we see is the governance, the policies, and many of those procedures and laws that actually makes it easy for entities to work together and really foster that business and that digital economy. And this is where we definitely encourage everybody to come and really learn from that model. All of these pillars helped us to counter many of the cybercrime, and as a matter of fact three major threats that we focus on in UAE. One is cybercrime, as the maginger of many

of those cybercrimes, comes from financial or monetary type of aspects, and but nonetheless, there is cyber tourism where sideolgies comes in data perspective as well as misinformation, dysinformation, radicalizations, many of those comes as well together in order to affect or impact many much our infrastructure. And then the cyber welfare where critical infrastructures are built and invested on and we need to make sure that we protect all of these investments, and this is where definitely the collaboration with many governments as well as vendors and industries to help us to come into that same mission where we protect and we provide many of that resiliency. Academia as well, it's another mageer things that we use in order to foster that encouragement of leveraging and using cybersecurity. Academia, there are so many universities that are actually focusing on building that and design security in many of the products and curriculums that they have. Security and design is one of the most and major important things that we always encouraging, and definitely working together with many of those entities.

The major aspects that I want to end with is the cybersecurity culture. We need to spread that cybersecurity culture across all sectors that we have. That's our goal and this is why we created many initiatives that was that. One of them is the cyber policy that we are presenting as well during this great summit. Thank you very much.

>> KAREN MULBERY: Thank you. Next is a remote participant ICT Postal and Courier Services in Zimbabwe. Dr. Jenfan Muswere. Is he online?

>> JENFAN MUSWERE: Thank you very much. I'm permanent secretary of postal and Courier services representing the Honorable Minister that could not join us. Let me start by uploading ITU for putting us together on this WSIS Forum to discuss very critical issues in as far as the development of ICTs is actually concerned.

>> KAREN MULBERY: I'm sorry. Let me ask you your questions or the Minister's questions and then you can respond. So we can get those on the record. The two questions I have for Zimbabwe is what is the role of legislation in building confidence and security in the use of ICTs? What laws has Zimbabwe put in place to build confidence and security in the use of ICT within the country? Thank you.

>> JENFAN MUSWERE: Thank you very much for those very important questions. If you recall a long time ago in 2002. 16th ITU Plenipotentiary Conference held in Morocco, and that is Member Countries we formally acknowledged that the benefits of ICTs could only be fully harnessed if there was confidence, and that these technologies and networks were reliable, secure, and

could be trusted when we trans act.

As we work towards attainment of the Sustainable Development Goals, the preservation of the digital benefits of digitization in ICTs means that we have to minimize the attacks, the cyberattacks on networks used for both social and initial communication. This is more important post this COVID era where ICTs are becoming an int dpral part of our lives and where new technologies are emerging, technologies such as artificial intelligence, Blockchain, IoT, et cetera, et cetera.

The overall legislation is to reduce the economic social and political impact of cyber threats, and some of these threats are -- we need to protect against children online, and we also need laws to regulate how we trans act unequalness, and also need to ensure that the privacy of all of our citizens is guaranteed. We need data protection laws for our corporate space, and such other organizations, as well as cyber laws for our security of states.

Zimbabwe, specifically, has not been left behind in trying to build laws to protect ourselves against the Cyberspace. In that regard, we have the criminal law fortification and reform act which contains a totally dedicated chapter on computer crimes. We also have the children's protection act, Chapter 5.06 which sets out children's rights and also protection against any vices targeted at children.

We have recently promulgated the cyber and data protection act which has amended some of the existing laws to provide in detail the parameters for data processing in disclosure as well as the procedures to be followed in the rules that govern responsible for data protection in both the public and private sector.

You've been trusted to know that Zimbabwe is continuously reviewing the ICT policy framework to take on both ongoing ICT developments and emerging cyber risks and is in the process of enacting the electronic transactions act. As a country, we are fully cognizant that we're part of the international community. We are a significant tree to several international and regional conventions and treaties and we therefore commit to harmonize our cybersecurity initiatives with those of the region, where we are, Africa, and the world at large to increase international cooperation in the fight against cybercrime. I thank you.

>> KAREN MULBERY: Thank you very much. Next we have the Honorable -- Ambassador for Digital Affairs ministry for Europe and foreign affairs from France. How is France committed to promoting a framework for the responsibility behavior of different actors in the use of information and communication technologies? And could you tell us about France's initiatives in the terms of cyber capacity building? Thank you.

>> HENRI VERDIER: Thank you very much. As a French dip mat I will speak French. We have a very good tradition. So we're dealing now with essential things. We've been working on digital for a while now because I created my first company in 1995, and I would like to remind you that risk or any weaknesses in the ITU world or the are of some people or some states and unprecedented so we do need a very important commitment to guarantee security of Cyberspace, and of course the behavior of all of the stakeholders is important, for instance committed to that in a multilateral commitment. We do work on different processes with the UN, and I'm just back from New York where we're a working group has been set to improve our understanding of the international law and the way we can apply it to Cyberspace., also the UN charter and -- so it requires a lot of work.

And within these multilateral processes, France with other colleagues such as Egypt, think that it's not enough to act in a responsible way. We have to make sure that we can implement our premises to this way in the UN we are working on the action plan to have staff dedicated to the implementation of responsible behaviors with two very important topics, with the promotion of building of (?) because some issues are related to the poor infrastructures we work in and with, and we do have to promote the work of the state actors because if you want that, 195 countries are safe on the Cyberspace, we do need some solidarity so that everyone could benefit from the skills.

Now we've got a third dimension. We cannot only count on state actors. We have to act in a responsible way and it goes for the society and private sector. So you will remember the call for Paris for Cyberspace with more than 70 states, 800 companies, 1,000 NGOs and we do work together on the new responsible behavior, and we have worked on a different dimension which is a non-state behavior, such as the nonproliferation or any action we can implement on this matter.

So to answer the second question, we do work a lot opt capacity building as much as we can, and some -- we've got some staff dedicated to the scientific investigations and cooperations, and for two topics we particularly brought up, so we've got the cyber national call in Senegal and there is another school in Montenegro which has national certification for the Balkan countries.

>> KAREN MULBERY: Next is Dr. Velislava Hillman. Do you see any long-term challenges as a result of the quick digitalization of education with respect to privacy and security? And what must we do to build confidence and security within the education-technology arena and ensure children's rights and best interests are met? >> VELISLAVA HILLMAN

thank you, Ms. Mulberry. Excellencies, distinguishes delegates, it's a honor to be here and thank you for the invitation and it's a honor to be here and shed light on the challenges and increasing challenges to education systems globally. I'm a researcher in the School of Economics and lead the organization called Education Data dij Dij kal Safeguards which engages with education companies to hold the industry accountable for impact to education.

The long-term challenges, while acknowledging the opportunities that the technologists tried for us are beyond cybersecurity. Digital technology advancement leaves governments generally inadequate about the challenges in digitizing education, and broadly speaking, the challenges are made from understanding in depth the risks that emanate from exploititive data practices in privacy laws, cyber insecurity, and also the impact of advancing algorithmic systems for inferencing and prediction. This leads Ed tech education companies and big-tech companies in charge of what happens in education. While education broadly still has state sovereignty, government priorities remain within the citizen.

If the sovereignty is lost and governance veers into the hands of the private sector, priority, we need to remind ourselves that priorities remain with their own business. We can view the issues from stakeholder perspectives or education community, and the challenges are relating to data privacy laws, data collection for profiling, digital surveillance, cyber insecurity is also continuing to grow in magnitude and frequency, and special needs, low-income children and individuals from LDCs can be especially vulnerable in this fast-paced digitalization.

At the Pedegoic level and not forget that it's still providing systems and personalized learning that helps teachers and students. There is evidence that teachers can be sidelined with actual pedagogy handed over to advancing algorithmic systems. And from the sector perspective, there are many opportunities that digital technologists can afford, absolutely, however there is lack of consensus around what standards benchmarks, frameworks, guidelines the companies have to adhere to, and how do companies guarantee and demonstrate data privacy and security, or that they prioritize children's best interests and fundamental rights.

So, what do we do to build confidence and security long term? A combination of two things should happen and we address government official, representatives, technology companies here and online. One, we must prioritize education over market well-being through top-down regulation, comprehensive governance, and clear consensus around frameworks, benchmark,

and standards and independent audits for building that kind of trust, transparency, and accountability.

Enforcing mechanisms are also needed to certify that the sector follows clear rules, protocols, and standards. Working together with teachers, within the decision-making process and digitalization of education is crucial. Lastly, the research and education communities do excellent work in providing evidence, and this should be encouraged, and they should collectively continue to build and demand evidence from Ed tech companies, from big techs as well. Thank you.

>> KAREN MULBERY: Thank you very much. Next Mr. Stephan sprk Duguin. CEO of cyberPeace Institute. According to the cyberpiece institute what are securities and what regulations and practical can you share?

>> STEPHANE DUGUIN: Thank you very much. On behalf of the CyberPeace Institute it's a privilege to address and thanks for the invitation and organizers. The CyberPeace Institute is independent and neutral Swiss Foundation headquartered here in Geneva, and our mission is to protect the most vulnerable in the Cyberspace, and I would like to use these minutes to talk about them, the most vulnerable in Cyberspace.

I guess everyone here knows the theory that you cannot protect anyone in Cyberspace until everyone is protected because of the inter-connected aspect of Internet that we want to safeguard at all costs. It's important to focus for a second on the ones with the least capacity to defend themselves against the ones with the most of capacity to attack them.

And we would like to talk about this critical organization, which are directly contributing to the realization of the Sustainable Development Goals, by assisting and protecting people throughout the world. We're talking about UN agencies, about international organization, but as about thousands and thousands and hundreds and thousands of NGOs which are on the frontline to provide humanitarian relief, support, and activate development agenda.

So cyberattacks have taken place against large international organizations, and I'm pretty sure you heard about these in the United Nations the International Committee of the Red Cross, but as it's less known, NGOs such as Save the Children, Merce Corps, Lots of Peace, impacted by cyberattacks. 2003, Geneva and plan of action that sets forth commitments and promotion of sustainable development, and that in building the information society, we shall pay particular attention to the special needs of marginalized and vulnerable groups of society.

I think that's in mind, and we need to remember that more than 1-billion people across the world receive digital support and services from these NGOs and safeguarding these NGOs against

cyberattack becomes priority especially when the world is moving crisis to crisis, climate to health care, to geo-politics.

So we emphasize and advocate for collective approach to cyber resilience in development and humanitarian sector and recognizing these needs, the CyberPeace launched on the 27 of February this year the humanitarian cybersecurity center.

With the center, hosted and developed within Switzerland with the ambition to offer platforms on the local level to have global reach, we provide for free cybersecurity to the NGOs, free incident, post-incident, so that the ones with the least capacity can be secure and get help when it's the most needed. We provide tools, support expert, for free assistance to NGOs tailored to their needs through partnership and networks. And I will emphasize this in front of this audience, this works only through partnership and networks. This humanitarian cybersecurity center is a platform where public sector, private sector, academia, Civil Society can join forces and incubate and invest into product and services for free which will help NGOs to reach this maturity cybersecurity level, again for the theory that as long as everyone is not secure, no one is. Thank you very much for attention. Pleasure to be here.

>> KAREN MULBERY: Thank you very much. The next panelist is -- excuse me. Professor Salma -- excuse me. Salma -- I'm sorry, my throat is dry. From the eWorldwide Group. Yeah.

>> SALMA ABBASI: Good afternoon, your excellencies, ladies and gentlemen. Let me begin by introducing myself. My name is Professor Salma Abbasi and Founder and Chairperson of e-worldwide Group and thank madam Secretary-General Doreen Bogdan-Martin and Gitanjali and the team for organizing this important event and inviting me to this important high-level panel and policy discussion.

As we rapidly integrate emerging technologies, AGI, Chat GBT, VR, 5 G, 6G, Web 4.0 and 5.0 into every sector, governments need to examine the effectiveness and safety of the entire ecosystem to ensure that regulations, law, and standards and collaboration frameworks are resilient, and more importantly that the knowledge is continuously being updated and relevant. We are living in times where we willingly allow surveillance in our home through a series of smart devices listening to private discussions without paying any real consideration as to who is in control, where does the data go, ornd understanding how the invisible space is governed just for our convenience.

The impact is even more serious for the youth and feature of humanity and our societies. As they socialize online through multiple social media platforms, gaming and gambling sites, often blindly signing the terms and conditions, they are unaware

and unknowingly handing over data to unscrupulous players buying and selling and profiling their every online move, categorizing, exploiting, and selling it.

We have now become the product, and are continuously being bombarded with information, nudging, grooming, manipulating our thoughts, invisibly by nefarious characters to fulfill their own agenda commercial or otherwise.

This has given rise to a new breed of global social media influencers who have become digital role models without substance, validation, or ethics. These people are dramatically impacting the impressionable young minds especially our children trying to mimic unhealthy behaviors, risky behaviors, unhealthy lifestyles, changing physical appearances, following fads and unsafe challenges, and adopting negative ideology.

The youth are actually determining their self-worth and popularity through the number of likes they have on their posts and followers. This is having a devastating impact on the self-esteem, confidence, mental health, causing depression, and in some cases suicide.

This has also given rise to the FOMO phenomenon, fear of missing out. Social media addiction. We are engaged with youth around the world for the last year and a half, building holistic human digital resilience, and in that context, I'm happy to share that the youth collectively believe that it's the government's responsibility primarily regulators, to keep us safe online.

An example of this can be seen in the UK where following the tragic death of the 14-year-old Molly Russel in 20007, who viewed self-harm content and subsequently committed suicide, this was deemed the cause by the corner, and the father has dedicated his life to drive comprehensive understanding of this cause and created an online harm bill which has resulted in great collaboration across multiple ministries, education, justice, health, social services, home affairs and other stakeholders and not just the ICT ministry, and more importantly, recently, the IEEE in collaboration with Barnes Kidren and other stakeholders developed the new standard of age-appropriate digital service framework which we are now operationalizing in the UK.

But it can be easily localized to any country that wishes to do so.

In conclusion, it's imperative to governments to develop mechanisms to monitor the ungoverned online space across the entire ecosystem to determine authentication accountability, conformity, compliance, transparency, and governance in collaboration with multisector stakeholder. This complex, multi-faceted situation -- one minute -- requires innovative and

global cooperation and collaboration and continuous consultation to address the evolving threats and risks, not only on the Internet but in the dark web and the deep web. These are dynamic times, and requires an understanding of the lived experiences. It's only through such models of collaboration and cooperations with governments that they'll be able to build confidence and trust in the digital environment to keep us safe. Thank you so much.

>> KAREN MULBERY: Thank you. The last panelist is remote, Dr. Olga Cavelli, director of the South School on Internet Governance. Are you with us, Olga?

>> OLGA CAVALLI: I'm here. Can you hear me?

>> KAREN MULBERY: Let me ask the question. Which are the main actions that developing countries and governments should implement to creator a safer cybersecurity environment? And which are the main challenges for developing countries in relation to cybersecurity?

>> OLGA CAVALLI: Thank you. Thank you, Karen. Nice to see you, virtually. It's been a while, we haven't met. My name is owinga Cavalli, currently the national Director of cybersecurity in Argentina and Director of Suite School of Internet Governance and thank you for having me with the high-level authorities and congratulations to ITU and WSIS Forum for a great new event of the WSIS Forum.

According to the World Economic Forum it is estimated that the shortage of cybersecurity professionals is more than 3-million globally and more than half a million in Latin America and Caribbean. The lack of cybersecurity experts and lack of cybersecurity knowledge in general brings problems to the opportunities offered by the digital economy, particularly for developing countries that need to achieve sustainable growth and trust-building environment.

One of the biggest challenges for developing economies in relation with cybersecurity is to implement concrete regulatory steps to establish some relevant elements to create a safe security environment. Having a national cybersecurity strategy is a foundation, although having it established does not solve all of the cybersecurity issues, it helps to create a safer environment and the main rules and considerations that a nation must have implemented or planned to prevent incidents.

The national cybersecurity strategy of Argentina has made established by the national executive branch of the government and established the guiding principles and develops the central objectives that makes it possible to set the rules for the protection of Cyberspace.

And in my role as National Director of Cybersecurity of Argentina I'm considering that cybersecurity is a permanent

change in environment, and open public comment period for the community to give their inputs to the next second cybersecurity national strategy.

Argentina has also established a specific regulation towards national administration organization, and makes it mandatory for the national administrations to establish a cybersecurity plan and to have a focal point in order to inform the national CSIRT for national cybersecurity incident that may occur. One of the important issues of cybersecurity is creating awareness and building capacity in the community and within all the stakeholders. Countries need to understand the need to create awareness and culture associated with security of information that allows them to understand the implementations related with the threats and the objective of legal protecting them by establishing legitimate legislative functions.

As an academic, I am the Director and Co--founder of South School for Internet Governance a program features Internet policy issues to fellows who participate in the program. In the program cybersecurity and cybercrime are one of the highlights of the activity program. The school offers free fellowships for training in Internet governance in a 6-month program that includes online pre-training, hybrid face-to-face capacity building, and of research phase that again, achieving university diploma. Fellows complete the three stages of the university diploma and what created by universe of Mendoza and available in Spanish, English, and Portuguese and received championship WSIS prize 2022. Many thanks for your attention and having made this opportunity. Thank you.

>> KAREN MULBERY: Thank you very much. This time I would like to thank all of our panelists for their participation, their comments, and their insights into what's happening with security so that we can gain our trust in ICTs and get a sense of what the governments are doing to not only collaborate with each other but to work with their citizens to establish that trust and respect.

Thank you very much.

(Applause).

***

***