IEEE EXPERTS IN TECHNOLOGY AND POLICY (ETAP) FORUM

on Internet Governance, Cybersecurity, Privacy, and Inclusion

Windhoek, Namibia, Africa

30 May 2017

IEEE INTERNET INITIATIVE

Version: 20 July 2017

IEEE INTERNET INITIATIVE

Contents

Executive Summary

The IEEE Internet Initiative, in cooperation with IST-Africa, on 30 May 2017 hosted an IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity, Privacy, and Inclusion in Windhoek, Namibia. The first IEEE ETAP Forum in Africa, the event preceded the IST-Africa 2017 Conference and engaged 65 technology developers, policy makers and other stakeholders from 25 countries.

A series of invited speakers laid the groundwork for further discussion at the IEEE ETAP Forum by exploring the issues, barriers and opportunities associated with achieving a safe, secure, trusted, affordable internet for all—a key enabler of the United Nations Sustainable Development Goals (SDGs)—especially across the African continent. Working groups then formed around the main challenges and opportunities identified by participants, more deeply considered their respective issues, proposed next steps and made plans to continue progress online following the Windhoek gathering.

Introduction: IEEE Internet Initiative and IEEE ETAP Forum Series

The IEEE Internet Initiative promotes innovative solutions for a trustworthy and inclusive internet by contributing technical expertise and resources to global and regional policy discussions and providing a platform for collaborative development of action-oriented and implementable outputs. The initiative:

- Monitors and assesses the potential impacts of technology developments related to the internet to make it more accessible and trustworthy
- Connects technologists with policymakers and other stakeholders to identify highest-priority issues and develop associated action plans
- Collaborates to develop and implement regional internet-advancement roadmaps that support an inclusive, safe, and trustworthy internet

The IEEE ETAP Forum on Internet Governance, Cybersecurity, Privacy, and Inclusion series is one of the primary vehicles through which the IEEE Internet Initiative carries out its work. The events facilitate uncommon collaboration among the world's technology developers seeking a better understanding of the public-policy landscape for the internet and policy experts globally seeking reliable technical guidance for more informed decision making—all toward the goal of advancing technology for the benefit of humanity.

They are "a series of events to have local conversations on a global scale, bringing the public, private, government, academic and research, societal, and funding sectors together to discuss issues and opportunities in the areas of internet governance, cybersecurity, privacy, and inclusion," said Dr. Maike Luiken, vice chair of the IEEE Internet Initiative policy track.

It was the seventh IEEE ETAP Forum but the first in Africa following gatherings in North America, the Middle East, and Asia:

- San Jose, California, in the United States in May 2015 (http://sites.ieee.org/etap-sanjose/)
- Tel Aviv, Israel, in August 2015 (http://sites.ieee.org/etap-israel1/)
- Washington, D.C., USA, in February 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-washington-dc)
- Delhi, India, in March 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-delhi-india)
- Beijing, China, in May 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-beijing-china)
- Tel Aviv in June 2016 (http://internetinitiative.ieee.org/events/etap/etap-forum-in-tel-aviv-israel)

Working groups subsequently explored and produced white papers on some of the priority issues

raised at these forums:

- Options and Challenges in Providing Universal Access
- Protecting Internet Traffic: Security Challenges and Solutions
- Internet of Things (IoT) Security Best Practices
- Algorithmic Decision Making

The IEEE ETAP Forum in Windhoek continued the discussions within the context of a theme of "Cybersecurity: Combatting cyber crime while advancing internet inclusion for all."

Invited Speakers

"While we embrace the open ecosystem of the internet, we should also be cautious that it gives powers to cyber criminals," said Mr. Nhlanhla Lupahla, Deputy Director: Innovation, Ministry of Higher Education, Training, and Innovation, Republic of Namibia, in opening the IEEE ETAP Forum in Windhoek. "Hence, the potential consequences of a realized cyber threat are extensive, and that has catapulted cybersecurity into the boardroom—thus, the rationale for this forum today."

Mr. Lupahla cited "significant progress … made in Africa over the last seven years in increasing cybersecurity awareness and putting the necessary legal and implementation frameworks in place." He noted a range of milestones including the 2011 establishment of AfriCERT to enhance cybersecurity of African countries through more effective collaboration and communication and launch of cybersecurity policies and computer incident response teams (CIRTs) in Cameroon, Uganda, South Africa, Mauritania, Egypt, Mauritius, and Kenya.

After Mr. Lupahla's welcoming remarks, four invited speakers delivered presentations:

- Prof. Basie von Solms, Centre for Cyber Security, University of Johannesburg, South Africa
- Ms. Elizabeth Kamutuezu, Acting Deputy Director: IPRM, Ministry of Information and Communication Technology, Namibia
- Dr. Towela Nyirenda-Jere, Principal Programme Officer, NEPAD Agency, South Africa
- Mr. Njei Check, Agence Nationale des Technologies de l'Information et de la Communication, Cameroon

Prof. Basie von Solms: Cybersecurity Awareness (CSA) in Africa

Prof. von Solms issued a call to action for substantially expanded cybersecurity awareness across Africa. The need is urgent, he said, because of an unfolding mobile-phone explosion on the continent, which is set to transform how public services are delivered and business and politics are conducted.

"Citizens of this continent are more and more … not forced, but empowered to use their mobile phones," Prof. von Solms said. "We must look at the cons; what are the consequences? The big thing is the increase in cyber crime. Ladies and gentlemen, let's not be naive about this—we are going to see more and more cyber crime ... because we leverage the mobile so much."

He noted a 2017 report (https://www.standardmedia.co.ke/business/article/2001235820/kenya-worst-hit-in-east-africa-by-cyber-crime) that African countries lost at least $2 billion in cyber attacks in 2016. Losses to cyber criminals included $171 million in Kenya, $85 million in Tanzania, and $35 million among Ugandan companies.

Increasing cybersecurity awareness, Prof. von Solms said, is a key, cost-effective part of the solution and has been shown to measurably reduce risk. Programs should be distributed broadly among

citizens, users, non-governmental organizations (NGOs), companies, and government departments, he said.

While he said there are some success stories, such as at the Centre for Cyber Security (CCS) at the University of Johannesburg (www.cybersecurity.org.za), efforts must be more sophisticated, he urged, proposing creation of an Africa-wide, standardized "Introductory Course for Cybersecurity Awareness."

"Because I'm from Africa, I know too well that we are very, very good at creating policies and legal systems and laws, etc., etc., but many of those are not executed," Prof. von Solms said. "… Africa is crying out for comprehensive cybersecurity awareness programs."

Ms. Elizabeth Kamutuezu: Internet Governance and Cybersecurity in Namibia

Ms. Kamutuezu said about 72 percent of Namibia's population of 2.1 million people enjoy access to the internet, though only about 53 percent have broadband access.

She detailed the Namibian landscape of information and communications technology (ICT) and cited a number of key achievements in enhancing cybersecurity to protect information infrastructure and ensure that the internet is safe for its growing numbers of users in the country. Achievements include establishing a Namibian Internet Governance Forum (IGF) working committee and working toward establishing a national CIRT. In addition, toward the goal of safeguarding the republic's security and economic wellbeing, the Namibian government has drafted the Electronic Transaction and Cyber Crime Bill to address problems pertaining to safety and security of digital communications of any mode.

But the challenges, Ms. Kamutuezu said, are substantial and myriad:

- The IGF is not a formal decision-making body.
- Cyber crime is borderless.
- The legal and regulatory framework to ensure cybersecurity is lacking.
- There is a shortage of information, statistics, and records of cyber crime committed in Namibia due to absence of laws, lack of capacity, and general awareness of cyber crime.
- Public/private institutional collaboration lags.
- Systems are poorly designed and managed.
- Social networking is on the rise, and increasingly cyber crimes are perpetrated through the social networks.

Ms. Kamutuezu urged for greater public advocacy and awareness, continued buildout of a conducive legal environment, institutional capacity building, and harmonization of national and international regulations. Also, for the good of the republic, the Namibian government must work more closely with companies to ensure the effective implementation of cybersecurity policies once enacted, she said.

Ms. Kamutuezu closed with a challenge for the IEEE ETAP Forum participants to consider the balance between security and privacy.

"Both are very, very important," she said. "We need security for our people, but our people also have their own rights … Where do your rights end and others' start? We need to strike that balance."

Dr. Towela Nyirenda-Jere: Cybersecurity and Multi-Stakeholder Internet Governance - The Case of the AU Convention on Cybersecurity

Dr. Nyirenda-Jere advocated for broad collaboration across African Union (AU) member states encompassing civil society, government, private sector, and academic representatives in a multi-stakeholder approach to cybersecurity and internet governance in Africa. At the same time, she outlined the challenges of such an approach in the context of a case study of the AU Convention on Cybersecurity and Protection of Personal Data (AUCC).

She cited the 2005 World Summit on the Information Society "Tunis Agenda for the Information Society," which read in part, "We encourage the development of multi-stakeholder processes at the national, regional and international levels to discuss and collaborate on the expansion and diffusion of the Internet as a means to support development efforts to achieve internationally agreed development goals and objectives, including the Millennium Development Goals."[1]

Dr. Nyirenda-Jere noted challenges to such a vision, including the lack of a universal agreement on the means of interaction and engagement among the various stakeholder groupings. She spoke on the perceived dominance of the different groups in multi-stakeholder processes (media, civil society, academia, and the technical community tend to be "less visible" than government), as well as the challenge of reconciling basic differences in "the ways of being and doing" among the different players. Also, she said, discourse occurs both online and offline, introducing both pros and cons in terms of participation and reach.

She stepped through the five-year process leading to 2014 adoption of the AUCC, intended to harmonize e-legislation, protect personal data, promote cyber security, and fight cyber crime. The AUCC covers electronic transactions, personal data protection, cybersecurity, and cyber crime and would set a series of requirements for member states:

- Develop national cybersecurity policy
- Develop legislation on cyber crime
- Ensure the protection of critical information infrastructure
- Enact personal data protection laws

Dr. Nyirenda-Jere described reaction to the AUCC—that the document is generally held as a good guideline/benchmark, which both promotes adherence to national constitutions and international human rights law and emphasizes the African Charter on Human and Peoples' Rights. On the other

[1] http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

hand, she said, “there are concerns around some of the provisions, which may be too vague or broad and may actually provide loopholes. And there are some concerns that the convention doesn’t define clearly the minimum thresholds that governments must adhere to.”

Also, she said, there is an inconsistency in that racism and xenophobia are outlawed but discrimination on sexual orientation and gender is not. Plus, she said the AUCC does not provide safeguards on information sharing between the private sector and government.

While Benin, Cape Verde, Comoros, Congo, Guinea Bissau, Mauritania, Sierra Leone, Sao Tome and Principe, and Zambia have signed the convention, she said, ratifications have lagged—one in 2016 and one through June 2017. Fifteen are required for “entry into force.”

Dr. Nyirenda-Jere closed with a series of questions for reflection about multi-stakeholder processes in light of the case study of the AUCC:

- What are the limits of multi-stakeholder approaches?
- Are such approaches really feasible/practical?
- What are the roles and responsibilities of the various actors and stakeholders?
- Who needs to do what, when, how, and why?
- How long should the process take? Can we afford lengthy ratification processes?

Mr. Njei Check: Implementation of a Framework to Support Cybersecurity and Internet Governance in Cameroon

Mr. Check discussed the appeal of digital economy and broadband access as catalysts for innovation, competitiveness, and gross domestic product (GDP) growth in Cameroon but also the threats posed by cyber theft. He presented a range of statistics detailing cybersecurity-related losses in Cameroon from 2012 through 2016:

- More than $8 million (U.S. dollars) loss incurred through scamming and phishing
- More than $7 million loss incurred through skimming
- Registration of more than 300 cases of spoofing social-network profiles and blackmail
- More than $400,000 loss incurred through intrusion
- More than $25 million loss incurred through SIMBOX fraud
- 28 web-defacement attacks perpetrated against public-administration websites
- More than 12,814 vulnerabilities detected on public-administration websites
- Law enforcement received more than 150 requests related to cyber criminality

Cameroon’s government has developed a legal and regulatory framework to help fight against cyber crimes, Mr. Check said. Elements of the framework include awareness training and capacity building, CIRT, security audit, digital certification/public key infrastructure (PKI), and management of internet resources (-.cm and Internet Protocol addresses), as well as enactment of laws on electronic communications, cybersecurity, and cyber crime which punish intrusion into information systems, denial of service, and privacy-related attacks. Also, the National Agency for Information and

Communication Technologies, “ANTIC,” was reorganized, and a special fund to finance cybersecurity-related projects was created.

Mr. Check detailed a range of next steps for Cameroon:

- Improve on sensitivity to cybersecurity and capacity building
- Reinforce the national CIRT
- Construct a backup for the national PKI
- Construct a national government data center
- International recognition of secure socket layer (SSL) certificates issued by Cameroon’s PKI
- Accredit private companies to carry out security audits
- Improve on the development of local content
- Reinforce the legal and regulatory framework
- Promote migration from IPv4 to IPv6

“It’s a huge challenge,” Mr. Check said. “It is imperative for each country to take cybersecurity with a lot of concern … and reduce insecurity to an acceptable level.”

Review of Previous IEEE ETAP Forums, Goals for Forum in Namibia

Dr. Maike Luiken discussed the IEEE Internet Initiative's role in bridging stakeholder communities and providing a collaborative platform for advancing solutions and informing global technology policymaking through a consensus of sound technical and scientific knowledge in internet governance, cybersecurity, privacy, and inclusion. She also summarized the top issues raised at the previous IEEE ETAP Forums (Appendix IV) and detailed the goals for the gathering in Windhoek:

- Engage local government officials, organizations, business, and industry in sharing and discussing the issues, barriers, successes, and opportunities to achieve a safe, secure, trusted, and affordable internet for all
- Foster interaction among stakeholder communities
- Arrive at an understanding of local priorities
- Determine next steps and form working groups
- Provide a forum report to forum participants and stakeholders

Working Group Report Summaries

The IEEE ETAP Forum next moved into working group meetings and reports. Participants voted on a range of potential topic areas for working groups (Appendix III) and then divided among one of the five focused conversations:

- Combatting cyber crime while maximizing internet inclusion for all
- Public awareness and education on internet safety and cyber crime
- Trends in cyber attacks and cyber crime
- Data protection, privacy, and resilience in the era of Internet of Things (IoT)
- National CIRT development

"We put a program on each of the tables with some questions," Dr. Maike Luiken said. "They're guidelines. This is *your* working group—not ours."

Working groups were asked:

- What is the current situation on this issue in your countries?
- What has already been done (success stories and good practices) in your countries?
- What is the goal/vision? What would you like to see happen?
- What are your current challenges?
- What are your proposed next steps?

Following their meetings, the working groups each presented comprehensive reports of their responses and input to the questionnaires, as well as additional contributions.

Combating Cyber Crime While Maximizing Internet Inclusion for All

What is the current issue in your countries (political, social, technical, and technological)?

- Government restriction on accessing internet/social media for political reasons
- Social networks allow impersonation and bullying
- No social guidelines on social-media use
- Lack of technical skills to prevent and respond to attacks
- Balancing the need to secure internet access with protection of individual rights

What has already been done?

- Policies and regulations in place or in progress
- Cybersecurity awareness and education
- Funding for cybersecurity interventions

What needs to be done?

- Internet education from homes
- Training for parents to train their kids on cybersecurity
- Combat ICT illiteracy
- Policies and laws that clearly define cyber crime, irrespective of cultural background
- Training for teachers in primary schools and high schools in a form of coaching and mentoring, in order to overcome computer phobia
- Addition of cybersecurity training to all computer courses
- Capacity building

What are the current challenges and opportunities?

- User ignorance
- "I don't care" attitude
- Fear of using the internet
- Lack of an integrated approach to cybersecurity at regional level
- Opportunities for collaboration through seminars, conferences, and workshops and educational partnerships across regions

While internet connectivity must be expanded, the group said that a more sustainable approach is needed; for example, enough people must be trained to prevent and/or respond to cyber crime.

The group discussed the need to instill a culture of cybersecurity in young people, as well as to personalize cybersecurity education patterned to the devices people are using. Additionally, the group identified the need for shared language on cybersecurity among policymakers and teachers. Also, they said, when a computer or mobile device is purchased, the buyer should receive a copy of a cybersecurity clause (with terms and conditions translated into an easily understandable document), and the buyer should acknowledge that he/she has read it.

Public Awareness and Education on Internet Safety and Cyber Crime

Two tables of participants addressed this issue, and responses from both groups have been collapsed into the following report.

What is the current situation on this issue in your countries?

Table A reported:

- Namibians are not wholly aware of cyber crime, and, therefore, public awareness is highly recommended. National CIRT establishment is underway and is seen as the central driver for public awareness. Namibia needs a consolidated effort from all stakeholders.
- Malawi is about to establish the cybersecurity strategy under the Malawi Communication and Regulatory Authority.

- Kenya is at greater cybersecurity risk because of use of mobile money. Kenya has established cybersecurity strategy and a CIRT to mitigate the advance of cyber crime.
- South Africa has immense needs for public awareness, which should be addressed in primary and secondary curricula. South Africa has about four CIRT organizations, and the public is not aware of what they are doing.

Table B reported that, overall, awareness is very low to low in all countries except Kenya, which was rated as average for multiple reasons:

- Government agencies heavily promote the importance of cybersecurity awareness, as most (if not all) of Kenya's e-government services are provided online (e.g., eCitizen was advertised via radio, TV, internet, etc.)
- Some institutions offering internet services have campaigns around safe usage (e.g., MPesa).

What has already been done (success stories and good practices) in your countries?

Table B reported that most of the countries have cybersecurity laws in place and that the remaining ones are working toward enacting laws. The participants detailed their assessment in the following table.

Namibia	Draft bill in the making Mitigations have been made to address cyber-crime issues that have already happened
South Africa	Cybersecurity bill was passed
Kenya	Existing "Computer and Cyber Crimes bill" in place
Malawi	Cybersecurity strategy in place Electronic Transactions and Cybersecurity Act 2016
Ethiopia	Cyber crime and e-Signatures law has been approved Professionals have been trained to train civil servants from all sectors Information and network security agency sends out SMSs on how one can protect data
Senegal	Cybersecurity law in place Ratified the AUCC
Tanzania	Cyber crime law passed since 2015 There are government agencies that deal exclusively with cyber crime issues (including police force, judiciary, and Tanzania Communication Regulatory Authority) TCRA has cyber-crime response team

What is the goal/vision? What would you like to see happen?

Table B reported that its vision would be to have zero cyber crime and maximum awareness. It said it would like to see:

- Increased public awareness for all citizenry
- Reinforcement and monitoring of policy frameworks on cybersecurity
    - Need for implementation of strategies and policies (not just talk)
- Government commitment to sustainable funding toward cybersecurity

What are current challenges and opportunities?

Table A reported:

- There is a great demand for awareness on the continent, as per participants from Kenya, Namibia, Malawi, and South Africa.
- Citizens do not understand their rights and limits.
  Relevant audits are lacking.
- Law enforcement agencies face challenges about cyber criminals without legal instruments.

Table B reported:

- Government as a stakeholder lacks understanding of the threats posed by cyber crime.
- Information from important forums regarding cyber crime and cybersecurity is not shared with all citizens.
- Skill development for certified information-security professionals in cybersecurity awareness is lacking.
- Critical mass of trainers to address cybersecurity issues does not exist.
- There is no civil society involvement and engagement.
- There is a lack of political will.

What are the next steps?

Table A proposed:

- Reusing what is available and roll out to schools, government employees, law enforcement, and citizens to create awareness and reduce cyber crime
- Formalizing structures to ensure accountability and responsibilities
- Ensuring availability of national budgets for cybersecurity initiatives
- Encouraging regional and continental bodies to consolidate these points with their plans
- Contacting IEEE to ensure correct authorities are engaged

Table B proposed:

- Efficiently piggybacking cyber crime awareness with a huge drive toward public understanding of science and technology
- Educating relevant stakeholders
    - Train the trainers
    - General awareness
    - Special/targeted groups (e.g., policymakers, politicians, judiciary, etc.)
- Utilizing media (radio, SMS, churches/mosques, newspapers, public forums, chiefs, etc.) to more easily reach more of the population
- Leveraging peer learning in which countries could learn from each other (and adapt to the local context)
- Translating existing curriculum to local languages (localization)

Trends in Cyber Attacks and Cyber Crime

What is the current situation in your countries?

- South Africa
    - Cyber crime is a big problem in South Africa, as a victim, as a perceived perpetrator, and as a safe haven.
    - There is a growing body of research into how South Africa is affected by cyber crime from the private sector and also from cybersecurity companies.
    - The South African Cyber Crimes and Cybersecurity Bill is in parliament and is about to be debated.
- Namibia
    - Namibia is No. 1 in cyber crimes and cyber attacks in Africa, according to research.
    - There is insufficient cyber policy for working on the cyber attacks and security.
    - There is much research done in Namibia about cybersecurity.
    - There is no automated system working properly in Namibia; techniques are outdated.
    - Not enough procedures are in place to combat cyber attacks. A bill in the parliament is being debated.
- Sudan
    - Cyber attackers are still improving their procedures (social media, phishing, etc.)
    - The government has implemented a department for combating cyber attacks.
- Uganda
    - The country has no specific law for combating cyber crimes, but a National Information Security Policy and framework exist.
    - Uganda needs greater awareness of cyber crimes.
    - Cyber attacks are common to banks, though many are not reported.
    - A response team under the CERT UG, which is under the National IT Authority, and UgCERT, which is under the Uganda communication commission, share a primary aim to monitor and respond to cyber-crime issues.
    - Plans are underway to have cyber laws and strategies to control attacks.

- Botswana & India
    - Much work has been done across academia, the military, and the financial community.
    - Making laws requires substantial effort.
    - Financial losses in India have been substantial.
- DR Congo
    - Sim-box attacks are prevalent.
    - There is no monitoring of voice over Internet Protocol (VoIP) calls.
    - No law is in place covering cyber crime.
    - Laws related to the implementation of post and telecommunications exist.

What has already been done (success stories and good practices) in your countries?

- Policies are in place to combat cyber crimes.
- Bank transactions are monitored (in India, South Africa, and Namibia), and the amounts that can be transacted are limited.
- Cameroon has established a national Cyber Auditing Organization.

What is the goal/vision? What would you like to see happen?

- Catching cyber crime while it is happening
- Profiling of individuals/organizations, their actions, and activities (via policies, international cooperation, and technology improvement)
- Sharing cyber-crime experience
- Continuously communicating cyber crimes within communities
- Establishing cyber/IT auditing organizations

What are your current challenges and opportunities?

- Organizations don't like to share their information because of privacy issues.
- Investments in cybersecurity are insufficient.
- Making life easier via IoT implementation exposes internet to threats.
- There is a lack of political will for implementation of new technology
- Communication between IT professionals and other stakeholders is hindered by ICT terminology and the rate of growth of technology.
- There is a conflict between privacy and security (encryption).

What are your proposed next steps?

- Stipulating guidelines on how to filter information that comes through the internet
- Creating national budgets for fighting cyber crimes and attacks
- Implementing cyber-crimes policies and laws
- Continually improving cyber-crimes laws and skills
- Moving from IPv4 to IPv6
- Providing standardized cyber-crimes awareness courses via universities

In addition, the working group said that more research would inform industry/government teams that are globally responsible for educating communities about possible cyber attacks.

Data Protection, Privacy, and Resilience in the Era of Internet of Things (IoT)

What is the current situation on this issue in your countries?

- Data Protection
    - Stakeholder interaction level (Swaziland)
    - Extended challenge of data privacy and protection (Rwanda)
    - Technology rollout is ongoing at a faster pace than legislation (Egypt)
    - Cyber-crime bill in progress (Namibia)
- Privacy
    - Nothing has been done at the government level, though some initiatives have been undertaken in the private sector (Swaziland, Namibia, and Tanzania).
        - Thrust on smart grid and especially smart agriculture
    - Despite privacy issues and other major concerns, there is a plan to deploy 250,000 smart meters (Egypt).
- IoT
    - Companies have started using IoT, especially in sugarcane farming, such as for monitoring moisture, machinery, etc. (Swaziland)
    - IoT is too huge; the domain of applications, too diverse across smart homes, smart homes, agriculture, etc. (United Kingdom)
    - Industry 4.0 is becoming a huge project (European Union)
    - Digital-manufacturing elements (Africa)
    - Smart cities, fiber to the home (Egypt)

What is the goal/vision?

- Government policy and legislation before focusing on technical aspects
- Policies and legislation that explicitly spell out data ownership
    - Who owns the data?
    - Which rights do owners of that data have?
    - What is the data being used for?
- Building trust for the acceptance of the technology and transparency
- Open data initiatives

What are the current challenges and opportunities?

- Infrastructure and energy for powering devices
- Layered security
- Increasing attack vector
- Weighing negative social impact against positive social gain
- Harmonized legislation for cross-border issues

- Spectrum regulation
- Capacity to enforce policies and legislation
- Applicability of blockchain toward solution design

What are the proposed next steps?

- Balance between awareness and resilience
- Address need 24/7/365 availability
- Identify strategic partners in driving technology uptake
- Address need for a policies and regulation framework
- Determine priority application areas
- Balance between privacy and data protection
- Achieve end-to-end security in a generalized way and specific to particular domains

National Computer Incident Response Team (CIRT) Development

What is the current situation on this issue in your country?

- Namibia
    - National CIRT established a steering committee
    - CIRT yet to be incorporated in the draft bill
- Lesotho
    - Computer Crime and Cyber Crime (CCCC) Bill awaiting approval
    - CCCC Bill will set the ground work for the committee
- Cameroon
    - Established the CIRT, currently in revision stage
    - Law on cyber crime and cyber criminality enacted since 2010

The working group noted that 12 African countries have established CIRTs, of which three are Southern African Development Community (SADC) member states.

What has already been done (success stories and good practices) in your countries?

- Namibia
    - Stakeholder engagement
    - Draft ICT Bill in place, to incorporate CIRT integration
- Lesotho
    - Computer Crime and Cyber Crime Bill approval
- Cameroon
    - CIRT in place
    - National Cyber Crime Strategy in place

What is the goal/vision? What would you like to see happen?

The working group identified its goal as to have a vibrant, responsive cyber team that is trusted, collaborative, and reliable. The working group's vision is of secure cyber space in Africa.

What are the challenges and opportunities?

- Namibia
    - Placement and hosting of the CIRT
    - Absence of an enabling act
- Lesotho
    - Approval of the bill
- Cameroon
    - Reinforcement of legislation in place

What are the next steps?

The working group proposed benchmarking and collaboration.

Next Steps and Wrap-up

Dr. Maike Luiken closed the IEEE ETAP Forum by noting the event's terrific geographic diversity (25 countries represented). She also pointed out that it was the first IEEE ETAP Forum to be sponsored by the IEEE Internet Initiative in partnership with another organization—in this case, with IST-Africa. "One plus one when you're partnering always adds up to more like three, four or five," she said.

Dr. Luiken said the IEEE Internet Initiative would be following up with the working groups formed at the event and, furthermore, would not forget the other topics raised at the forum that were not selected as areas of focus for working-group discussion at the forum. She especially encouraged participants who feel called to engage in one of those other areas to reach out to the IEEE Internet Initiative.

Finally, she thanked participants for the "energy and commitment in the room … and your dedication to a better internet for all."

Join the Conversation

The IEEE Internet Initiative is a cross-organizational, multi-domain community that connects technologists and policymakers from around the world to foster a better understanding of, and to improve decisions and advance solutions affecting, internet governance, cybersecurity, privacy, and inclusion issues. There are many ways to engage through the IEEE Internet Initiative. Please visit http://internetinitiative.ieee.org or email internetinitiative@ieee.org for more information.

Appendix I: Program

Date: 30 May 2017

Location: Safari Hotel Conference Centre, Windhoek, Namibia

Theme: "Cybersecurity: Combatting cyber crime while advancing internet inclusion for all"

Start Time	End Time	Program
10:00	11:00	Registration and Coffee
11:00	11:10	Welcome Participants
11:10	11:20	Welcome Address Mr. Nhlanhla Lupahla, Deputy Director: Innovation, Ministry of Higher Education, Training and Innovation, Namibia
11:20	11:40	Cyber Security Awareness (CSA) in Africa Prof. Basie von Solms, Centre for Cyber Security, University of Johannesburg, South Africa Professor SH (Basie) von Solms is a Research Professor at the Academy for Computer Science and Software Engineering at the University of Johannesburg in Johannesburg, South Africa. He is also the Director of the Centre for Cyber Security at the University of Johannesburg and Associate Director of the Global Cybersecurity Capacity Centre of the University of Oxford in the UK. Professor von Solms specializes in research and consultancy in the area of information and cybersecurity, critical information infrastructure protection, cyber crime, and other related cyber aspects. He has written and presented more than 130 papers about these fields—most of which have been presented at international research conferences and/or published in international subject journals. In addition, he has supervised more than 120 post-graduate students in the ICT field. Professor von Solms is a past president of the International Federation for Information Processing (IFIP). He is a Fellow of the Computer Society of South Africa, a Fellow of the British Computer Society, a Chartered Information Technology Professional (CITP), and a member of the editorial boards of the International Journal for Business and Cyber Security. His personal home page is at http://adam.uj.ac.za/~basie.

Start Time	End Time	Program
11:40	12:00 pm	Internet Governance and Cybersecurity in Namibia Ms. Elizabeth Kamutuezu, Acting Deputy Director: IPRM, Ministry of Information and Communication Technology, Namibia Elizabeth Ujarura Kamutuezu is currently Acting Deputy Director for Institutional Policy Regulation & Monitoring, Directorate: ICT Development in the Ministry of Information and Communication Technology. Her main responsibilities involve providing professional and/or technical support in the undertaking of comprehensive research and analysis on different issues relating to information and communication technology (ICT) policies and the functioning of government, aimed at achieving coordination and harmonization of functions, programs, and projects. She also assists in formulating policies for the government through the MICT with respect to information and communication service provisioning and technology and infrastructure development and maintenance in Namibia. She was the national coordinator for the Namibia Digital Terrestrial Television (DTT) migration, through which Namibia successfully attained a 72% population migration. She served as a board member of the Namibia Internet Exchange Point (IXP). She is a member of the Internet Governance Forum Working Committee. Elizabeth Ujarura Kamutuezu has more than 15 years of experience in development planning and policy analysis. She obtained a Bachelor of Economics from University of Namibia in 1998, majoring in economics and management science; a Bachelor of Philosophy (Hon) in sustainable development planning and management from the University of Stellenbosch in 2010; a Graduate Diploma in leadership development in ICT and knowledge society in 2013 from Dublin City University; a Master's degree in leadership development in ICT and the knowledge society from the University of Mauritius in April 2017; and is currently busy finalizing her MBA in international business at Amity University, India.

Start Time	End Time	Program
12:00	12:20	Cybersecurity and Multi-Stakeholder Internet Governance - The case of the AU Convention on Cybersecurity Dr. Towela Nyirenda-Jere, Principal Programme Officer, NEPAD Agency, South Africa Dr. Towela Nyirenda Jere works in the Regional Integration, Infrastructure and Trade Programme at the NEPAD Planning and Coordinating Agency as a Principal Programme Officer focusing on policy, legal, and regulatory aspects of infrastructure and services. She has over 15 years of experience working in the private sector, academia, and currently in international development. She initiated the NEPAD Internet Governance Programme, helped to launch the Southern Africa Internet Governance Forum, and co-founded the African School on Internet Governance. She represents NEPAD on the ICANN Government Advisory Council and served on the IGF Multi-Stakeholder Advisory Group in 2014 and 2015. She holds a PhD in electrical engineering (networking and telecommunications) from the University of Kansas, a Master of Arts in contemporary diplomacy (internet governance), an ACCA Diploma in financial management, and is a qualified project management professional (PMP) with the Project Management Institute (USA). Towela is a member of the Malawi Institution of Engineers, the Internet Society (ISOC), and the Institute for Electrical and Electronics Engineers (IEEE). She also serves on the IEEE ad-Hoc committee on Africa activities. She continues to advocate for increased awareness among African policy makers of the importance and significance of infrastructure and ICT development, internet governance, and policy processes at national and continental level.
12:20	12:40	Implementation of a Framework to Support Cybersecurity and Internet Governance in Cameroon Mr. Njei Check, Agence Nationale des Technologies de l'Information et de la Communication, Cameroon Njei Check currently heads the Security Audit Division of the National Agency for Information and Communication Technologies (ANTIC), Republic of Cameroon. He has led over 30 security audit missions for information systems in both public and private organizations in Cameroon. He also played an important role in the development of Cameroon's public key infrastructure and actively worked on the development of e-government strategy and national security policy for Cameroon. He participates in the organization of the annual Internet Governance Forum in Cameroon, where he presents issues and solutions related to cybersecurity on the internet. He has also participated in several international conferences to present research on e-government and the security of information systems. Njei has more than 14 years of experience in ICT solution development. He was instrumental in establishing various skills in software development, innovation, project management, and strategy development in the complex governmental environment. He manages ICT-related projects that have been implemented across several government agencies. Njei (Msc. in computer engineering, National Advanced School of Engineering-Polytechnic Yaounde, 2004) has earned several credentials, such as Project Management Professional (PMP), COBIT, ITIL, and ISO 27001. He had a fellowship at United Nations University/International Institute for Software Technology in Macao, China from March 2010 to October 2010, and he has attended several training programs both in Cameroon and abroad.

Start Time	End Time	Program
12:40	12:55	Panel Q&A
12:55	13:15	Working Group Topic Selection Participant Introductions – Name, Affiliation, Country, Most important topic for Working Group discussion
13:15	14:00	Lunch
14:00	14:15	IEEE Internet Initiative - Mission and Goals; Review of Previous ETAP Forums; Goals for ETAP Namibia Dr. Maike Luiken, Vice Chair, Policy Track, IEEE Internet Initiative
14:15	14:25	Working Groups Breakout Participants move to their chosen working group tables
14:25	15:30	Working Group Discussions – Current Status & Practices
15:30	15:40	Coffee Break
15:40	16:40	Working Group Discussions – Desired Future & Path Forward
16:40	17:50	Working Group Reports
17:50	18:00	Forum Wrap-Up
18:00	20:00	IEEE Internet Initiative Reception

Appendix II: Participants

The following individuals attended the Windhoek IEEE ETAP Forum on 30 May 2017:

Mauridi Abubakari, COSTECH, Tanzania
Olabode Samuel Akinsola, NUST, Namibia
Leulseged Alemie, Ministry of Communications and Information Technology, Ethiopia
Fungai Bhunu Shava, Namibia University of Science and Technology, Namibia
Njei Check, National Agency for Information and Communication Technologies (ANTIC), Cameroon
Paul Cunningham, IIMC, Ireland
Miriam Cunningham, IIMC, Ireland
Peacemaker Dlamini, Department of Science and Technology, South Africa
Mbuso Dlamini, RSTP, Swaziland
Emilia Eino, Ministry of Information and Communication Technology, Namibia
Mohammed Elbasheir, Sudan University of Sciences and IT, Sudan
Licky Erastus, Namibia University of Science and Technology, Namibia
Karin Fröhlich, DPSITM, Office of the Prime Minister, Namibia
Attlee M. Gamundam, NUST, Namibia
Aminata Garba, Carnegie Mellon University, Rwanda
Augetto Graig, Republikein, Namibia
Ndafapawa Haimbala, Office of the Prime Minister, Namibia
Haitham Hamza, Information Technology Industry Development Agency (ITIDA), Egypt
Joris Stani Ikany-Mpemba, Namibia University of Science and Technology, Namibia
Flora Ismail Tibazarwa, SAIS II, Namibia
Imaja Itulelo Matiyabu, University of KwaZulu-Natal, South Africa
Gloria Iyawa, University of Nairobi / UNISA, Namibia
Gift Kadzamira, National Commission for Science and Technology, Malawi
Elizabeth Kamutuezu, Ministry of Information and Communication Technology, Namibia
Cisse Kane, ACSIS
Chipo Kanjo, University of Malawi, Malawi
Ebenhezer Kauhonina, National Commission on Research, Science and Technology, Namibia
Maike Luiken, IEEE, Canada
Nhlanhla Lupahla, Ministry of Higher Education, Training and Innovation, Namibia
Sagwadi Mabunda, University of the Western Cape, South Africa
Paul Macharia, Ministry of Health, Kenya
Ntombi Mchuba, Department of Science and Technology, South Africa
Ivan Molefe, Communications Regulatory Authority of Namibia (CRAN), Namibia
Elly Mulilo, Ministry of Information and Communication Technology, Namibia
Moses Muundjua, Namibian Standards Institution, Namibia
Loi Namugenyi, Uganda National Council for Science & Technology, Uganda
Lakshmi Narasimhan, University of Botswana, Botswana
Patrick Ndayizigamiye, University of KwaZulu-Natal, South Africa
Ndeshipanda Ndilula, Office of the Prime Minister, Namibia
Rauha Ndjambi, Ministry of Health and Social Services, Namibia
Jacob Njagih, Ministry of Education, Science and Technology, Kenya

Augusto Nunes, INTIC, Mozambique
Towela Nyirenda-Jere, NEPAD Planning and Coordinating Agency, South Africa
Diarmuid O'Briain, netLabs!UG Research Centre, Makerere University, Uganda
Cecilia Onyadile, SADC, Botswana
Flavia Oums, Uganda Bureau of Statistics, Uganda
Thomas Owens, Brunel University London, UK
Ndahekelekwa Paulus, Office of the Prime Minister, Namibia
Anicia Peters, Namibia University of Science and Technology, Namibia
Ariel Phiri, IEEE Zambia Section Vice Chair, Zambia
Phodiso Phole, Ministry of Transport and Communications, Botswana
Gernot Piepmeyer, National Commission on Research, Science and Technology, Namibia
Icconies Ramatsakane, PwC, South Africa
Sam Rametse, SKA SA, South Africa
Paul Rowney, AfICTA
John Scheffers, Namibian Standards Institution, Namibia
Ashwin Seegolam, National Computer Board, Mauritius
Paulus Sheetekela, University of Namibia, Namibia
Saraphina Simeon, Office of the Prime Minister, Namibia
Josaphat Tjiho, YALI, Namibia
Diana Tjirare, Namibia University of Science and Technology, Namibia
Lieketseng Tjokotsi, Department of Science and Technology, Lesotho
Martin Ujakpa, International University of Management, Namibia
Basie von Solms, University of Johannesburg, South Africa
James Wendorf, IEEE, United States
Panayiotis Zaphiris, Cyprus University of Technology, Cyprus

Appendix III: Top Identified Issues

Voting on possible topics for working groups at the IEEE ETAP Forum in Windhoek, 30 May 2017:

- Combatting cyber crime while maximizing internet inclusion for all, 7 votes
- Balancing privacy concerns while combatting cyber crime, 3 votes
- Multi-stakeholder internet governance, 0 votes
- Public awareness and education on internet safety and cyber crime, 18 votes
- Developing/operationalizing legal frameworks and strategies related to national cybersecurity, cyber crime, and internet governance, 4 votes
- Trends in cyber attacks and cyber crime, 7 votes
- Data protection, privacy, and resilience in the era of Internet of Things (IoT), 9 votes
- National Computer Incident Response Team (CIRT) development, 8 votes
- Developing critical information infrastructure protection frameworks, 2 votes
- Security audits of information systems in public administration, 3 votes
- National Public Key Infrastructure (PKI) development, 0 votes
- Digital currency – possibly replacing national currencies, 2 votes

Appendix IV: Combined Issues List, All IEEE ETAP Forums

Windhoek, 30 May 2017

- Combatting cyber crime while maximizing internet inclusion for all
- Public awareness and education on internet safety and cyber crime
- Trends in cyber attacks and cyber crime
- Data protection, privacy, and resilience in the era of Internet of Things (IoT)
- National Computer Incident Response Team (CIRT) development

Tel Aviv, 22 June 2016

- What biometric data is appropriate for what circumstances?

Beijing, 17 May 2016

- Cyber-threats to critical infrastructure, including eGovernment/eCommerce
- Transparency as a source of obtaining data for evidence-based decision making
- Biodiversity in the Internet ecosystem

Delhi, 4 March 2016

- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Multi-stakeholder Internet governance
- Options and challenges in providing universal access for social and economic inclusion

Washington, 5 February 2016

- Data localization
- Education and ethics
- End-to-end security/privacy by design
- Technology-policy development process

Tel Aviv, 10 August 2015

- User assessment of trustworthiness of devices, enterprises, and governments
- Educating users about characteristics of information society
- Machine-readable privacy agreements and who enforces them?

San Jose, 18 May 2015

- Threats and opportunities in data analytics
- Multi-stakeholder Internet governance
- Protecting Internet traffic, managing meta-data analysis, and how to implement both security and privacy at scale
- Fragmentation of the Internet due to local policies and how to avoid it
- Algorithmic decision making that exacerbates existing power balances and ethical concerns
- How to best engage IEEE as a platform for contributing to the resolution of these and related issues