UGANDA INTERNET GOVERNANCE 2022 REPORT

The Uganda Internet Governance Forum (UIGF) is a multi-stakeholder meeting that brings together representatives from government, civil society, academia, technical community, private sector and individuals interested in Internet Governance (IG) issues. The objectives of the UIGF are to: Establish IG issues relevant to Uganda; Build consensus on national and regional positions around relevant IG issues and create awareness about various IG issues including online safety in Uganda especially among vulnerable users. Since its inauguration in 2006, the UIGF has continued to discuss and address Internet Policy issues pertinent to the country. To date, twelve (12) forums have been held with each addressing different thematic areas.

The 2022 Uganda Internet Governance Forum (UIGF) was on November 08, 2022 under the theme "**A Resilient and united digital inclusion for all Ugandans."** As in the previous year, the 2022 UIGF followed Uganda School on Internet Governance and the 2nd Youth Internet Governance Forum held on October 06, 2022 Sub-themes for the UIGF2022 included - Cyber security, data governance, privacy, digital inclusion, digital economy, Artificial Intelligence.

The one-day event brought together a total of 110 representatives from government, media, private sector, civil society and individuals interested in shaping discussion on how Internet can be used as tool for empowerment and development in Uganda.

The UIGF follows a bottom-up approach, which includes soliciting for topics from interested parties. The call for topics shared on different mailing lists and the forum website. The topics are then selected by a multistakeholder organizing committee comprising representatives from government, civil society and private sector to form the main theme and subthemes for the forum.

The UIGF 2022 was proudly sponsored by the Internet Society Foundation, Internet Governance Support Association (IGFSA) and the African Network Information Centre (AFRINIC).

Opening remarks:

Lillian Nalwoga, convener of the UIGF welcomed and thanks participants for participating in UIGF23. She urged members to actively participate in the internet governance process at the national, regional and global forum. She highlighted main achievements of the UIGF including developing the capacity of Ugandans in understanding IG issues through the Uganda School on Internet Governance (USIG) and the Uganda Youth Internet Governance Forum (UYIGF). She encouraged members to participate in the global IGF scheduled for December in Addis Ababa.

UYIGF 2023 Report presentation

A report from the Uganda Youth IGF was presented by Innocent Adriko, UYIGF Coordinator. The UYIGF 2022 was held on October 06, 2022 and attracted over 70 participants under the ***theme "Collective Youth participation in advancing Digital transformation and Inclusion"***

Key Highlights:

- Young people are agents of creativity and innovation, and can be drivers of change and transformation in their communities if meaningfully included in all processes.

- Youth need to get included in policy conversations as so as to be part of the decision-making process and contribute to reshaping Internet ecosystem in Uganda
- Importance of capacity building through offering free short courses to enhance knowledge on Internet Governance
- Having youth leaders taking centre stage in technology and Internet issues would be a step forward towards addressing challenges such as misuse of digital platforms and online crime. The digital gender

divide is also a challenge that needs to be addressed as females equally need to be included. See more here: https://livestream.com/internetsociety/uigf2022/videos/233685606

Keynote Address:

The keynote was delivered by Mr. Arnold Mugeni, Director of Information Security on behalf of the Executive Director Dr. Hatwib Mugasa. He highlighted importance of digital solutions in assisting revamping the economy post-covid 19. He further reiterated the importance of a safe and trusted digital infrastructure.

"A safe and trusted digital infrastructure is needed today more than ever." Mr. Arnold Mageni,

He shared that the government of Uganda through NITA-U implemented four phases of the national backbone infrastructure seeking to connect various places within the country. Through NITA-U, government has reached 62 districts and connected over 1400 entities that include the local governments, schools as well as hospitals. Through this, the end user is always the target group. He also shared that plans are underway to reach 80 districts and connect at least 3000 entities to the backbone. NITA -U is also working with other organisations Uganda Communications Commission (UCC), who have created a number of websites as well as connected a number of schools and the Rural Communication Development Fund (RCDF).

Government is also working with the private sector and also have developed a number of policies, and which has created fertile grounds for the private sector play as there's been a shift from leasing infrastructure from owning to leasing infrastructure, which has enabled small players to thrive in an environment that used to be capex intensive. That coupled with a number of initiatives including the National ICT support program, as well as other innovation leaning programs. That's created the financial muscle that is needed for start-ups, as well as for micro small and medium enterprises.

He also shared that that government aims to continue to build resilience by promoting safe and trusted public infrastructure. To this government has established the National Cybersecurity strategy as a guide towards ensuring that the National Information security framework which is aimed to give us protection or by spelling out the minimum-security controls that need to be put in place to give us a given degree of safety. Other initiatives include - the national CERT and Coordination Centre, to assist government response to cyber security incidents and provide early warming mechanism advisories amongst others. NITA-U has also been running October as the National Cybersecurity Awareness Month, where a number of promotional campaigns and materials are run to try and promote safe cyberspace usage in the country. Another campaign is the Se safe Online, which is a continuous initiative to try and promote the safe usage of ICT or digital infrastructure.

"We must be open even with those robots. We must be open to new technologies, because it's what will enable us connect ideas, economies cultures across the globe. These technologies will continue to change the way we work, the way we live and the way we interact. Since technology can never be free of vulnerabilities."

Arnold expressed concern about the global increase of global attacks both in number in sophistication and in impact. Noting a surge in the number of incidents, especially around ransomware as well as cyber theft, fraud and espionage which disrupts services. To this, he called for a change in our online behaviour to match the current global trends. **"If we don't change our behaviour online, then the cyberspace will only be hostile, where basic interaction and transactions cannot be trusted."**

He urged participant to be responsible users on the internet. ***"If we each do our part in our systems and devices and use our systems and devices responsibly, while putting in place reasonable security controls, then collectively we can promote cyber hygiene and help protect our systems and that term their own cyber-attack has brought a lot of motivation from various sources, collaborate to have access to sophisticated tools, and they don't respect jurisdictions."*** Arnold Mugeni.

He further called for the need to collaborations on cybersecurity initiatives so as to share experiences and capacity in order to address cyber threats and crimes. Cooperation and collaboration within the sector would increase resilience and improve capability to create a safe cyberspace.

Watch full session here

High level Panel: A Resilient and united digital inclusion for all Ugandans.

This session sought to address the importance of digital inclusion in Uganda. Questions raised included:

What needs to be done to help entrepreneurs adopt digital tools? Why is digital inclusion important when it comes to the internet? What digital rights issues arise when it comes to internet use in Uganda? Is the private sector using the proper methodology to have more women involved or avoid risk of having a gender war? How to attract and connect people to digital platforms in a sustainable way. What is the role of men and women in the future of digital business? Is government deliberate on ensuring no one is left behind? How do we build confidence in internet use?

Panellists included: Michael Bamwesigye, Head of Information Technology and Security, Uganda Communications Commission (UCC); **Japheth Kawanguzi**, Team lead, Innovations Village; **Robert Ssempala**, Executive Director of HRNJ-Uganda; **Peace Kuteesa**, Zimba Women Uganda; and moderated by**: Gabrie Iguma;** Restless Development.

Session highlights:

- Need to build competitive digital platforms for entrepreneurs in Uganda. Digital platforms need to be able to solve problems for people. There is also need to understand what can done to translate the opportunities presented by the internet into tangible results. That is what it is going to undertake to build strong competitive companies, companies that are resilient and attracting investments so as to create employment.
- Digital inclusion should not to be looked at as an issue of just including women, user diversity and equity in access is also important.
- Need to include youth and media into the digital inclusion
- Building digital skills for young people to be able to compete at a global stage

In order to unlock the entrepreneur innovation potential, a call for more private sector involvement in terms of venture capital where they can partner with the 'disruptive' entrepreneur was made. Entrepreneurs need to be provided with the right type of capital that will incentivise but also reward them as they hit growth milestones. Therefore, digital inclusion needs a multistakeholder approach that includes enabling private sector by incentivizing them go after problems that are traditionally known to be fixed by government. This will support in accelerating the rate at which opportunities are unlocked for the youth.

> ***"When it comes to building a strong digital economy, we need to build a policy environment that can incentivize intrapreneurs or can incentivize people want to invest in intrapreneurs? And then how do we get the private sector also playing in a more constructive way? For the benefits of the industry, they're in but also to unlock opportunities for a for entrepreneurs."*** **Japheth Kawanguzi**

Peace Kuteesa emphasised, "we cannot talk about inclusion and then leave out the fact that it's mainly women, because access to opportunities is different. Access to education is also different. You find that right from school, even the number of women who are enrolling in the tech space is much less than the women enrolled than men."

Cost of internet, ownership of devices and awareness of existing digital platforms plays a huge factor in closing the gender digital divide. Social norms also play a role in widening this divide. Many women in rural areas are unemployed which and cannot only afford internet but also don't own internet devices. The devices are owned by men who sometimes dedicate when they can use the device. Thus, when rolling out digital platforms, particular emphasis thus needs to be placed on ensuring that people who need to use these platforms have access to the Internet and can afford it.

> ***Internet use is governed by access to money, who has more money or who can afford the Internet? So, a lot of the women whether in rural and urban areas, get the money that they use for the Internet for maybe their husbands' brothers, fathers, so it's this woman gets a percentage of that income. So, the person who decides how much to give is the one who dictates how much Internet they meaning that that person probably has a lot they already like 10% ahead of you. Peace Kuteesa.***

Online safety especially for women is also another issue that causes the gender digital divide. Some of the safety concerns include targeted cyberbullying, lack of digital skills, among others.

Need to adopt gender digital policies that protect women as they use the internet. ethical guidelines on safety measures

Digital inclusion also means protection digital rights of online users. Some of the rights issues that mentioned include freedom of expression and privacy. Online users are constantly faced with challenges of cyber stalking and offensive communication. The current amendments within the Computer Misuse Act pose concerns to the enjoyment of these rights which may push people off the internet for fear of prosecution.

Session one: Advancing normative frameworks for responsible state behavior in cyberspace in Uganda

Panelists: Emmanuel Chagara, CEO Milima Security; **Dorothy Mukasa**, Executive Director, Unwanted Witness; **Arnold Mangeni**, Director Information security, NITA-U; **Prof. Rehema Baguma**, Makerere University; and **moderatored by Moses Owiny**, Centre for Multilateral Affairs.

A 2020 report of the Internet Governance's Best Practice Forum in relation to international cybersecurity agreements observed that not all established norm initiatives lead to policy changes. However, this does not indicate that these collective efforts are useless or unimpactful. Norms are not static products but socially dynamic processes, and their value stems from the processes themselves. The relevance of norms in fostering interstate peace and stability in the cyberspace is critical. It is now commonly known that governments are also behind cyberattacks, effectively using technology as a weapon against adversaries even in times of peace. Because of this, the potential for interstate conflicts and the risks associated with it is very high. For instance, in 2019 the accusation that the South African-based telecom company MTN Uganda was involved in abetting large- scale cyber espionage on the Ugandan government via its telecommunication networks led to the deportation of the top MTN management in Uganda by Ugandan authorities and strained diplomatic relations between the two countries. Incidents of state-inspired cyberattacks and cyber espionage have caused conflicts in both the online and physical spaces. Cyber threats undermine international peace and stability which is hinged on the efficacy of multilateral co-operation. Therefore, the need to institute co- operative measures such as norm development and implementation is more than necessary.

Key questions

Can the development and implementation of cyber norms provide stability as well as constitute a solution to bilateral and multilateral conflicts in cyberspace? How can norms be used to advance peace and stability in the cyberspace? How could norms developed at UN level be domesticated at national level? What roles do private sector, academia, technical community and government play in advancing this cause?

Cyber capacity building (both human & infrastructural) is key to critical network infrastructure protection but also the security of cyberspace. Can you elaborate on how these have been championed by the government through NITA-U? What areas of capacity strengthening are required? How resilient would you describe the security of network infrastructures within government bureaucracy? How can governments cooperate with each other either through CERTS/CIRTS to ensure interagency coordination to avert cybercrime, minimize state-sponsored cyberattacks and promote peace and stability in the cyberspace?

Session highlights:
The stability and security of the cyberspace is an issue that affects not just governments and multilateral agencies but individuals like us. Today we are confronted by issues of conflicts in cyberspace perpetuated by malicious actors, bad actors, but also governments. Right weapons of war even during times of peace, and this has, you know, issues and ramifications around you know, the protection and security of our critical Network.

Need to harmonize cybersecurity laws where addressing cyber security threats across boarder because as the norms require countries to support each other during investigations.

Privacy concerns need to address data security breaches to avoid abuse of personal data.

> **It should be mandatory, you know, government should make it mandatory for data collectors and service providers. For example, telcos to be able to do assessments periodically, i.e. assessment for, security of personal data should be a continuous process.** Dorothy Mukasa

Online users need to be empowered with information that relates to how their data is being so as to build trust with data collectors since technology is all about trust.

There is need to have a human rights centric approach to cyber security policy.

Data collectors and governments should have continuous dialogue with different stakeholders on how to secure their data.

Cybercrime is a borderless crime and its evolving very fast rate. The speed at which cyber threats are evolving is quite extensive and many institutions are grappling with the ability to respond to it. However efforts to address it are minimal. Besides, businesses are scared of the implications of security breaches especially when it comes to loss of credibility and non-compliance with the law. Institutions have to thus take a 360 approach when building strong cybersecurity controls. When talking about frameworks and norms, its importance to understand what are some of these frameworks that the private sector can rely on? Institutions also need to financially invest in build strong cyber security systems.

> **One of the key things is what are you going to suffer as an organization and some of them are faced with amongst others reputation damage. Now, quantifying the loss that you will face when your reputation is affected becomes difficult, because we do not have sufficient expertise to be able to do quantitative risk assessments.** Emmanuel Chagara.

Policies don't really stop crime, policies don't do much if the mindsets are still stuck in the wrong places.

Call to bridge the gap between those making policies and the people that are affected by these policies, through meaningful dialogue on how to best improve cyber security.

> You can have the best security in the world. But as long as the mindset is still upside down is not the way it's supposed to be i.e. not thinking. Is negative is selfish, is greedy, and all those bad things that make us deviate the standard norms of behavior. Security is a moving target. You're going to come up with a best technology today, but somebody else is busy coming up with another new a whole new attack that you had not thought about in this solution. – Dr. Rehema Baguma

Session two: Organizing to Resist: Impact of Shrinking Civic Space on Feminist.

Panelists: Bonnita Nyamwire, Pollicy Uganda; **Patricia Nyasuna**, Women of Uganda Network; **Carol Nyangoma Mukisa**, Warms Hearts Foundation; **Anthony Masak**e, Chapter Four Uganda; and moderated by Peace Oliver Amuge, Executive Director, Women of Uganda Network (WOUGNET)

This session sought to engage stakeholders including Feminists, Women Human Rights Defenders (WHRDs), Activists, civil society, the wider women's movement, Policy Makers, Internet providers and Communication Regulator. Discussions were informed by the evidence-based research contacted by the Women of Uganda Network (WOUGNET) in 2021 and the different engagements and experiences WOUGNET together with 20 civil society organisations have had as they work to promote online feminist organising in Uganda. It explored strategies, best practices from different countries on how to survive as feminist in the civic space that is currently shrinking plus an analysis of the legal frameworks that regulates online organising.

Session highlights:
Shrinking civic space entails three freedoms i.e. freedom of expression, freedom of peaceful assembly and freedom of association. Shrinking Civic space for women is mainly caused by the government due to unfavorable policy environment that affects Women their capacity to organise online. Some of the key obstacles faced by women when organizing online include online sexual harassments online usually caused by the men, arrests and intimidation of feminists due to their online activity and survillance.

Online gender-based violence in another issue faced by women when organising online which is leading to self-censoring themselves offline or online and do not want to share information anymore.
A call for capacity building and conducting research to document facts about status on shrinking civic space for women. Watch session here: https://livestream.com/internetsociety/uigf2022/videos/233685696

Session three: Bridging digital divide through a network of public and community libraries in Uganda.

Panelists: Asia Kamukama, Executive Director, Maendeleo Foundation,Uganda; Akia Mercy Prisca, Librarian, Soroti Public Library; Adonia Katungisa, Director, National Library of Uganda (NLU; moderated by Esther Kyazike, Kawempe Youth center

Session highlights
Libraries especially community libraries offer an environment for children and community members to interact with digital technologies while building digital capacity of community members. However, the high cost of data, language barrier, gender bias towards women using internet and inadequate IT infrastructure such as

computers are huge bottlenecks in running operations of community libraries. More about the session here https://www.eifl.net/events/uganda-internet-governance-forum-2022

Watch

https://livestream.com/internetsociety/uigf2022

Media coverage

https://youtu.be/0TLIDQZNW0w

- https://youtu.be/n9t-bIBw00A
- https://www.newvision.co.ug/category/science/telecoms-online-traders-warned-on-cybercrime-147065