LACTLD Report on IGF 2019

Berlin, Germany
25-29 November 2019
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Berlin IGF Messages</td>
<td>3</td>
</tr>
<tr>
<td>Security, Safety, Stability and Resilience</td>
<td>3</td>
</tr>
<tr>
<td>Data Governance</td>
<td>5</td>
</tr>
<tr>
<td>Digital Inclusion</td>
<td>5</td>
</tr>
<tr>
<td>Sessions of interest to the ccTLD community</td>
<td>6</td>
</tr>
<tr>
<td>IGF 2019 OF #6 ICANN: DNS, Threats and Opportunities</td>
<td>6</td>
</tr>
<tr>
<td>IGF 2019 OF #16 Collaborative Multistakeholder Approaches in Cybersecurity</td>
<td>7</td>
</tr>
<tr>
<td>IGF 2019 WS #331 Should we tackle illicit content through the DNS?</td>
<td>7</td>
</tr>
<tr>
<td>IGF 2019 WS #216 Online Identity in the Multilingual Domain Name Space</td>
<td>8</td>
</tr>
<tr>
<td>IGF LAC Space</td>
<td>9</td>
</tr>
</tbody>
</table>
LACTLD Report on IGF 2019

Introduction

The 14th Annual Meeting of the Internet Governance Forum (IGF 2019) took place in Berlin, Germany, from 25 to 29 November 2019, within the framework of the overarching theme: One World. One Net. One Vision.

During the course of five days, 3679 delegates participated in-person in 200 sessions. Berlin welcomed participants from 161 different countries. 53% of these were first-time comers and 42% of them were female.

The LACTLD Report on IGF 2019 features the most relevant Berlin IGF Messages around the three key themes of the IGF 2019: security, safety, stability and resilience; data governance; and digital inclusion. The report also examines some of the sessions of interest to the ccTLD community. It highlights the main discussions and policy recommendations that were identified at each of these sessions.

Berlin IGF Messages

Berlin IGF Messages are published on the official IGF website provided by the United Nations.

In order to reflect on the overall discussions held during the IGF 2019, a consolidated set of messages for all three key themes of the Fourteenth Annual Meeting of the IGF were developed. These messages are based on the post-session reports of the session organizers and live discussions that took place in Berlin.

Security, Safety, Stability and Resilience

This theme covers the vital role of cybersecurity, online safety, and stability and resilience of the infrastructure as prerequisites to economic growth and a healthy digital environment beneficial to all. It also deals with multistakeholder and multidisciplinary perspectives to protect both systems and users, gaining a better insight in the multidimensional aspects risks, threats and different ways to address them.

Another key aspect of this theme involves the stakeholder collaboration in responding effectively to the growing and rapidly changing range of threats to the global Internet and its users, while preserving the benefits all enjoy.

Messages on safety and security online

- The Internet will only achieve its potential as a channel of free speech and an engine for economic growth if it remains a safe place where people feel secure. Any cybersecurity approach must seek to preserve the benefits people enjoy while tackling the risks. This calls for holistic approaches to protect online users while building or keeping their trust in using the Internet.
Security and people’s fundamental freedoms and rights can coexist, but sometimes there need to be trade-offs. However, prioritizing security over people’s freedoms and rights, including freedom of expression and privacy, must be legitimate, proportionate, and based on the rule of law.

Discussions on online safety need to rely on robust data.

Achieving safety online requires involvement of stakeholders at different levels. Industry players and stakeholders should explore what is tangible and achievable when it comes to gathering and sharing information to prevent online abuse. Together, they could agree on ways to act and cooperate based on a shared understanding.

Messages on security of the infrastructure

While the current trend to tackle illicit or abusive content is to cancel, transfer, delete or suspend domain names via the Domain Name System seems like a quick and easy solution, it does not provide an effective and sustainable way to remove malicious content.

Online platforms and providers, while taking appropriate measures to delete or block illegal content, should also reach out to and cooperate with law enforcement agencies to provide information for preventive measures. Policy makers and responsible parties should gain more insight in the possibilities and limitations of technical measures solutions through collaborative multistakeholder partnerships.

More than a quarter of the Internet's traffic now runs on IPv6. Stakeholders need to continue engaging and collaborating, so that this important transition continues to happen.

Messages on policy and cooperation

The pace of technology development is outpacing traditional processes to put in place policy and regulatory processes to address security issues in a timely way. It is necessary to enhance collaboration to develop and implement policy solutions, and for norm development processes to be inclusive and respecting human rights.

Amidst the current atmosphere of escalating tensions between countries in cyberspace, resulting in the development of increasingly sophisticated cyberweapons, both defensive and offensive, it is ever more important to pursue effective confidence building measures (CBMs) to establish trust and promote global stability online.

Messages on capacity building

Internet users have an obligation to contribute to their personal security online. However, they can only be expected to act as responsible users if they understand what is at stake, are aware of the risks, know their rights, and have learned how to act. Users, in particular children, need to be empowered. Cybersecurity training and capacity building should
enable all users, including the more vulnerable groups and minorities, to become more secure online and able to demand and defend their human rights safely.

- Significant opportunities exist to improve the global ecosystem security through meaningful actions that promote trust and increase capacity among nation states, and between states and other stakeholders.

Data Governance

This theme deals with the role of data governance in fostering economic growth, innovation, social progress and sustainable development. Data governance discussions address how to best ensure the development of people-centric data protection frameworks at national, regional and international levels, as well as in related cross-border issues, that respects human rights, empowers individuals and promotes sustainable development.

The theme also covers the conditions and ethical frameworks needed to facilitate data-driven innovation while also ensuring fair competition, and fostering trust in the Internet and digital technologies.

Messages on cross-border data flows and development

- As data crosses borders, multiple legal and regulatory frameworks, such as personal data protection regulations, data disclosure requirements and judicial redress processes often apply, with the potential to produce uncertainty in global data-driven supply chains.

- Working collaboratively in a global context on developing commonly agreed values and principles for data frameworks could assist in building confidence in cross-border data flows, with resultant economic and social benefits.

Messages on data as the key resource of our economy and society

- Increasing uptake of Internet of Things (IoT) in urban infrastructure also inevitably results in more data being produced, collected and shared. It is essential to ensure public services are people-centric and data-driven, with participation and transparency in the design of services. Sustainable development and the protection of fundamental rights of all people, including marginalized groups, should be the overarching goals for policy making.

- A lack of adequate global and national human-centric data governance limits data’s potential as a key resource for sustainable development.

Digital Inclusion

This theme focuses on how digital inclusion sits at the heart of the IGF, reflecting the World Summit on the Information Society (WSIS) goal to build “a people-centred, inclusive and development-oriented Information Society where everyone can create, access, utilize and share information and knowledge”.

Messages on inclusive access to the Internet and its infrastructure

- Internet user growth has slowed down and connecting the unconnected remains a huge challenge. At the same time, attacks against Internet connectivity have become a dangerous instrument of politics.

Messages on social and economic inclusion, gender equality and human rights

- Bias and exclusion continue to be deeply imbedded in digital spaces. Discussion about inclusion of marginalized people should be at the centre of Internet governance and public policy conversations and not in the margins.

Messages on local content and language diversity

- The adoption of Internationalised Domain Names (IDNs) needs further encouragement and support by all stakeholders to increase the benefits made possible by having Internet domains in local languages and scripts but.
- Universal acceptance of IDNs and internationalized email addresses is not just a technical issue, it is also a policy issue. Governments and public entities should promote universal acceptance and lead by example through using IDNs themselves.
- Copyright can be both an enabler of local content production as well a barrier to content creation and distribution. Creative Commons licences give content creators control over how their content is shared and re-used.

Sessions of interest to the ccTLD community

IGF 2019 OF #6 ICANN: DNS, Threats and Opportunities

Theme: Security, Safety, Stability and Resilience
Subtheme: Cyber Attacks / Domain Name System / Internet Resources

The Open Forum focussed on ICANN’s 2020-2025 Strategic and Operational Plans. These Plans cover a series of issues such as security, DNS development, global development and improvement of the multistakeholder model of governance, with a focus on the potential of the DNS in terms of threats and opportunities. The session revealed great optimism about the future of the DNS (for instance, on issues related to IDNs growth) but also concern on the impact of DNS abuse; not least how it affects trust and confidence.

While no specific recommendations were defined, there was agreement on the importance of tackling DNS abuse across multiple fronts in order to enhance future confidence in the use and development of the DNS.

Session transcripts
Session video

IGF 2019 OF #16 Collaborative Multistakeholder Approaches in Cybersecurity

Theme: Security, Safety, Stability and Resilience
Subtheme: Capacity Building / Cyber Attacks / Cyber Security Best Practice

One of the main conclusions at the session was that cybersecurity challenges are broad and interrelated. Therefore, there is a need for inclusive and multistakeholder approaches in cybersecurity strategies.

During the session, many indicated that clear programmes and approaches should be put in place in order to assist the practical implementation of cybersecurity. Additionally, there was a lot of support for cybersecurity collaboration, capacity-building and capacity sharing.

Another key aspect of the discussion was the need to work more cohesively with law enforcement agencies and support police investigation and prosecution of cyber crime.

Some of the main policy recommendations and suggestions stated at the session were: capacity building of law enforcement agencies to collect and present evidence; raising users’ awareness of the cybersecurity threats; implementation of reporting mechanisms for cyber crime among users; strengthening cybersecurity for elections; promote collaborative work between cybersecurity experts and local communities in order to build effective strategies.

Session transcripts

Session video

IGF 2019 WS #331 Should we tackle illicit content through the DNS?

Theme: Security, Safety, Stability and Resilience
Subtheme: Domain Name System / Human Rights / Illicit content

This session was organized by NIC.br / CGI.br and LACTLD. Its panel featured representatives of the private sector, governments, technical community and civil society from Europe, Asia-Pacific, Africa and Latin America and the Caribbean.

At the beginning of the discussion, a distinction was made between deletion and suspension of a domain name. The speakers shared their perspectives on tackling illegal content at the DNS level.

Ms. Manal Ismail (Government, African Group) argued that in some circumstances there are legitimate reasons behind government demands for content removal.

Ms. Polina Malaja (Technical Community, Western European Group) recalled ccTLDs are just technical operators, with the responsibility of operating DNS infrastructures for their own TLD, as well as maintaining the registry database. She provided an overview of ccTLD responsibilities and experiences from countries of Europe that have chosen different approaches for solving DNS conflicts.
Mr. Thomas Rickert (Private Sector, Western European Group) said DNS manipulation may be mishandled by operators who disregard the most appropriate measures to remove contents. He emphasized that the issue should be correctly delimited, in order to provide the appropriate response, reducing the visibility of content, helping the victims and stopping abuse scenarios.

Mr. Miguel Ignacio Estrada (Technical Community, LAC Group) indicated reasons for not acting at the DNS level in order to solve problems related to contents, from technical to legal perspectives. He also stressed that brand owners are working to provide tools to legal professionals, so as to find those responsible for illegal online contents, instead of asking judges for taking down domain names.

Ms. Jennifer Chung (Technical Community, Asia-Pacific Group) raised a warning that illicit content may also be found in legitimate websites, so there is no way for a registry operator to surgically remove it. The options available for a registry are complete suspension, holding and/or removing it from the view, but those who have a record of the IP address may still be able to access that content. Therefore, registries cannot use their current frameworks to address this situation.

Based on the speakers’ contributions, a series of policy recommendations and suggestions were proposed during the session:

- Provide judges and prosecutors with information and appropriate tools so that they find those responsible for the contents.
- Help spread the word about the risks involved in taking actions at the DNS level and that host providers and content owners are the appropriate actors to whom the actions should be pointed out in the first place.
- Define clear thresholds to guide actions at the DNS level, as well as define some sort of chain of actions to be tried in first place.
- Foster more multistakeholder dialogue and collaboration so as to reach consensus solutions to diverse problems related to this debate.

Session transcripts
Session video
IGF 2019 WS #216 Online Identity in the Multilingual Domain Name Space

Theme: Digital Inclusion
Subtheme: Access / Digital Divide / Multilingual

The discussion at the session clearly demonstrated the problem faced by both those advocating for an Internet with diverse linguistic content and those involved in advocating for Universal Acceptance (UA).

Essentially, there is market failure as there is insufficient incentives for developers, operators or DNS players to make their systems UA/IDN friendly given the low take up for such names, itself because of lack of UA.
The session illustrated the problem, the mechanisms for addressing it and the focus needed on the public sector. It was identified that both a bottom-up and top-down approach is needed. In latter case, the use of standards is another potential vehicle for mandating service provision that recognises all domain names.

Session transcripts
Session video

IGF LAC Space

The IGF LAC Space had its fourth edition at IGF 2019. The meeting was organized by LACTLD and brought together more than 70 attendees, representatives of 22 organizations from Latin America and the Caribbean.

Participants representing technical community organizations and other stakeholders groups were able to share their updates and activities carried out during 2019, and also had the opportunity to present their projects for the coming year.

As in previous editions, the IGF LAC Space connected Latin American and Caribbean stakeholders and enhanced collaboration and cooperation activities across the region.

Session video