THE IGF IS A GLOBAL MULTISTAKEHOLDER PLATFORM THAT FACILITATES THE DISCUSSION OF PUBLIC POLICY ISSUES PERTAINING TO THE INTERNET

Workshop Proposals 2019

IGF 2019 WS #20 Empower young people to protect their privacy on internet

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
Internet ethics
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Government, African Group
Organizer 3: Technical Community, Latin American and Caribbean Group (GRULAC)

Speaker 1: Mamadou LO, Private Sector, African Group
Speaker 2: Chenai Chair, Civil Society, African Group
Speaker 3: Bignon Franck KOUYAMI, Civil Society, African Group

Policy Question(s):

What mechanisms to put in place to ensure effective awareness of young people?
How to make young people aware of the importance of responsible behavior online?
What mechanisms are in place today to ensure a secure and secure Internet for young people?

Relevance to Theme: This workshop is in keeping with the theme because it will allow us to reflect on the urgency of informing young users, especially African users, about digital hygiene and the protection of their data on the internet.

Relevance to Internet Governance: This workshop is part of the governance of the Internet because promoting Internet access for all without educating and raising awareness does not ensure secure internet access

Format:
Birds of a Feather - Auditorium - 60 Min

Description: A question-and-answer session with participants to initiate reflections on the need to raise the awareness of Internet end-users. For an hour of time, participants on site and online and speakers will have exchanges around the theme. Previous questions studied and prepared by the organizing team will be asked to the speakers for 30 minutes. the last 30 minutes will be free exchanges under the supervision of moderators

Expected Outcomes: - Raise awareness of this threat to young Internet users
- Talk about actions that are already taking place
- Share existing good practices

Discussion Facilitation:

This session will deal with a theme that affects youth. For once the session is validated, we will take the time to communicate on social networks to prepare participants online for the session. We will also provide a live tweet during the session in addition to using the official IGF platform.

Online Participation:

This official online plateform will help us to facilitate interactions between online participants and speakers.

Proposed Additional Tools: We are planning to also use Twitter with the official hashtag for the annoucement and during the session.

SDGs:

GOAL 4: Quality Education

IGF 2019 WS #22 Tackling hate speech: future regulation of intermediaries

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Hate Speech
Internet ethics
Trust and Accountability

Organizer 1: Government, Western European and Others Group (WEOG)

Speaker 1: Gerd Billen, Government, Western European and Others Group (WEOG)
Speaker 2: Chan-jo Jun, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Ingrid Brodnig, Civil Society, Western European and Others Group (WEOG)
Speaker 4: David Kaye, Intergovernmental Organization, Western European and Others Group (WEOG)

Policy Question(s):

What role should Internet platforms and governments play in defining the standards for acceptable content online in the light of freedom of speech? How can globally accepted standards be developed? Where is the middle ground between increasing demands for proactive content policing by digital platforms and the necessary neutrality and legal certainty for platforms?

Relevance to Theme: When the World Wide Web was developed in the 90's, hopes and expectations were high that it would be a space where people around the world could communicate freely and safely. However, in the last years it turned out that in particular social networks are often misused to distribute hate speech and that social networks are a place where harassment and bullying takes place. As a consequence, trust in the Internet was shaken. Although social networks in the first place denied their accountability for harmful third party content, governments and civil society urged them to remove harmful content from their platforms. In some cases social networks agreed to participate in codes of conduct, in others legislators introduced a legal framework social networks have to comply with. In this context, two aspects need to be observed: Firstly, measures need to be efficient to stop harmful content. Secondly, measures need to find a balance between the protection of human dignity and freedom of speech. If these rules are respected, trust in the Internet can be restored and accountability of the providers established.

Relevance to Internet Governance: At the centre of the debate is what the roles of governments, the private sector and civil society respectively are when dealing with the challenge of hate speech online. There are different views about who should be responsible to set the rules for keeping the Internet free from harmful content. The possible instruments vary from private standards over codes of conduct to legally binding rules.

Format:

Panel - Auditorium - 90 Min

Description: Participants: - Gerd Billen, State Secretary, German Federal Ministry of Justice and Consumer Protection (confirmed) - David Kaye, UC Irvine School of Law, UN Special Rapporteur on the Right to Freedom of Opinion and Expression (t.b.c) - Karine Nahon, Associate Professor, The Information School at University of Washington and the Interdisciplinary Center Herzliya (Israel) (t.b.c.) - Chan-jo Jun, Specialist lawyer for IT law (confirmed) - Ingrid Brodnig, author, activist and Journalist (confirmed) The workshop will begin with a presentation by attorney Chan-jo Jun, who rose to fame by supporting victims of hate speech online and instigating legal proceedings against Facebook. The other speakers will then have the opportunity to share perceived similar and/or different situations. The representative of the German government will then give a short overview about the Network Enforcement Act, and explain the reasons why the German Parliament passed the law, which introduced compliance obligations for social networks when dealing with complaints about illegal content online (Gerd Billen). The other participants will be asked to discuss other available instruments and strategies to fight harmful content. In particular, discussions will focus on what safeguards should be applied to secure freedom of speech (esp. David Kaye). Finally, it will be debated how chances stand to develop internationally accepted standards on how to deal with harmful content. During the workshop the audience will continuously have the opportunity to share their views and ask questions.

Expected Outcomes: A possible outcome could be the conclusion that it is a joint responsibility of all stakeholders to ensure a free and safe Internet from which harmful content is removed swiftly and effectively. However there will remain different opinions on what instrument will be the most appropriate to reach this aim. Nevertheless it should become clearer what is understood by harmful content and that there should be certain limits for the removal of content in order to preserve freedom of speech.

Discussion Facilitation:

An onsite moderator (still to be designated) will lead through the Workshop and will make sure that the audience can give their views and ask questions.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 4: Quality Education
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #23 How and why to involve perspectives of children effectively

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

Child Online Safety
Cyber Security Best Practice
Human Rights

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Leyla Nasib, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Phakamile Phakamile, Civil Society, African Group
Speaker 3: Daniela Beyerle, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

Why are children's views and experiences relevant to different stakeholders of the digital environment?
What responsibility do society, politics and business have for a good and safe growing up in the digital environment and the Internet?
What are good practise examples to involve perspectives of children effectively and responsibly?
Which tools and methods could enable companies and politics to better involve the perspectives of children and adolescents?

Relevance to Theme: Protecting children and young people from the risks and harm that the Internet and digital media can cause is indisputably important. However, to allow them to participate/engage in an age-appropriate and child-friendly way in developments and decisions that open up safe, creative and protected possibilities of using the Internet, is an approach that is still under-represented.
Governments, public authorities and businesses make decisions about conditions, rules and opportunities for using the Internet and digital media and content that must also take into account the best interests of children and young people.
Today, children are not only subjects to be protected from risks and harmful contents or experiences. They are not only consumers of media and devices. They are producers, readers, gamers and influencers, they have expertise, impact and power which can help understanding their views and changing policies in a human rights based and child-friendly way. Perspectives of children and youth are of course as different as the regions and cultures as well as the living conditions and chances of human beings. But children have the right to be heard in every issue they are affected of. That’s what the UN-Convention on the Rights of the Child (CRC) stands for and what has to be realised from the duty-bearers of the Convention – the States parties, the companies and all adult persons. The respect for and implementation of Children’s Rights has an essential dimension particular in digital contexts. At the same time, digitization offers a high potential for realizing to a greater extent the previously unrealized or under-implemented rights of children.
The right to access to mass media (Art. 17 CRC) , the right to privacy (Art. 16 CRC), the right to freedom of expression (Art. 13 CRC), the right to be protected from violence (Art. 19 CRC)– these are only a few dimensions, which open the view for discussions on this issue.

Relevance to Internet Governance: Mediatisation and digitization has led to a serious change in childhood and adolescent environments in recent years. The fact that digital media such as smartphones and tablets as well as the use of the Internet would soon find its way into many children’s hands or class rooms, was not foreseeable at the time of the resolution of the UN Convention on the Rights of the Child in 1989.
Nonetheless, Article 17 UN CRC makes it clear that States parties must allow children access to mass media and thus to "information and material from a variety of sources". Children's rights must accordingly come to their full development in the digital world. This means to take the views and experiences of children into account when discussing, developing and regulating the Internet in a worldwide context. But participation is not only a question of how to include perspectives in an equal and justice way but also how to guarantee fair and equal access to mass media at all.

Format:

Other - 90 Min
Format description: This workshop will be a combination of presentations and a tutorial. The session will

start with a short presentation of two international Best/Good Practices. During the second part of the session the participants will experience some of the methods and tools first hand. The tutorial will end with a moderated discussion about the participants' experiences and learnings.

Description: The workshop presents good practise examples for different ways of collaboration of companies or politicians with children. On the one hand, participants of the workshop can learn why perspectives of children and youth are relevant to consider in their own working context. On the other hand, participants can learn about and experience first-hand methods and tools that enable the participants to design and think from a „user's perspective".
The session will start with a short presentation of two international Best/Good Practices („Designing for children's rights guide" and „Web Rangers") that successfully managed to involve the children's and adolescences' perspective within their projects. The presentation is followed by a brief introduction into human centered design (minds & makers), explaining the „why" as well as the „how".
During the second part of the session the participants will experience some of the methods and tools first hand. In small groups they are invited to work with templates for e.g. personas or customer journeys and will present their results to the whole group. The tutorial will end with a moderated discussion about the participants' experiences and learnings throughout the session.
Agenda Outline
1. Presentation good/ best practice (15 min)
2. Presentation good/ best practice (15 min)
3. Presentation human centered design (15 min)
4. Interactive tool sessions in small groups and result presentations (30 min)
5. Reflections and discussion about the learnings (15 min)

Expected Outcomes: • Understanding of the importance and chances of involving children and adolescence effectively and responsibly
• Learning from and being motivated by international best/ good practices
• Brief understanding of human centered design
• Practical experience with using various tools and methods for involving children's and adolescent's perspective

Discussion Facilitation:

For the entire tutorial there will be a host. The host will introduce the topic and agenda as well as guide through the whole session. For the interactive part of the session we will provide templates and materials the participants are invited to work with. The participants will work in small teams, which stimulates a more intense exchange. The three speakers as well as the organizers will be part of the small teams and give their input if needed. For the closing discussion about the participants' learnings we will provide a structure and one of the speakers will moderate this part.

Online Participation:

We will inform people from our diverse network about the date and topic, format and policy questions of our workshop, that they are able to participate online to bring in their perspective and questions.

Proposed Additional Tools: Twitter/ Instagram: One of the organizers will moderate these channels during the session.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption
GOAL 17: Partnerships for the Goals

IGF 2019 WS #31 Digital Security and Human Rights in Tricky Landscapes

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Security Best Practice
Encryption
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Iryna Chulivska, Civil Society, Eastern European Group
Speaker 2: Kuda Hove, Civil Society, African Group
Speaker 3: Chirinos Mariengracia, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 4: Alp Toker, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

What are the changing threat models faced by human rights activists at the forefront of human rights, technology, and democratic advancement?

What tactics are human rights activists using to stay one step ahead of state and non-state threats and what are the policy implications? e.g.coping with internet censorship during times of national crisis

What is the impact of proposed legislation to confront online hate speech and how are governments using these laws to stifle free expression?

How do the threats in Sri Lanka, Ukraine, Venezuela, and Zimbabwe compare with international trends?

How can human rights activists leverage international support and attention to hold governments accountable for online attacks and deliberate network disruptions?

Relevance to Theme: The panel's focus will be on the technological resilience of human rights defenders' ability to cope with digital security threats arising from phishing attacks, malware, censorship, surveillance, etc. and the translation of that experience into policy remedies and advocacy.

Relevance to Internet Governance: The relevance to internet governance is our focus on policy remedies to mitigate attacks from state and non state actors. We'll discuss how pervasive digital attacks against human rights activists inform public policy development in at risk countries. We'll explore the inherent conundrum in trying to produce legislation that will place a check on a government's ability to carry out a cyberattack against its own citizens.

Format:
Round Table - Circle - 90 Min

Description: Security, safety, and resilience online are all prerequisites for citizens to effectively engage in civic activism online. When these attributes are tampered with by state and non-state actors to stifle civic activism, however, everyone's fundamental rights are put at risk. Unfortunately for most activists in non-permissive states, ensuring the online platforms on which they conduct advocacy are secure and resilient is a perennial struggle. Our panelists from Zimbabwe, Sri Lanka, Venezuela, and Ukraine all hail from different policy, political and security contexts, some more restrictive than others, but all struggle with protecting the

internet as a space for healthy, unfettered democratic activism. Our discussion will delve into each country context, how activists are working to stay secure online, and comparative practices in other regions. Our panel will explore the policy implications for keeping the internet secure and resilient in the face of threats to online rights. A technical expert from NetBlocks will discuss the various techniques governments use to manipulate and censor the internet and what the trend lines look like globally for online censorship. The format will be interactive and will encourage audience participation in order to surface new ideas for staying safe online while engaged in human rights activism.

Expected Outcomes: Our expected outcomes include exposing the IGF audience to the digital rights and security situation in four key countries, sharing new ideas from other civil society activists on confronting threats to security online, sharing regional trends and responses to online censorship, and to form and strengthen multistakeholder ties among the panelists and audience.

Discussion Facilitation:

We'll have a remote moderator onsite fielding questions and comments online, we'll be publicizing on each panelists' social media feeds, and the onsite moderator will promote remote participation throughout the panel.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: We'll largely focus on Twitter because that is where a disproportionate number of the IGF and digital rights community convenes.

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #41 Tech Nationalism: 5G, Cybersecurity and Trade

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)
Organizer 4: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Farzaneh Badii, Civil Society, Asia-Pacific Group
Speaker 2: William Hudson, Private Sector, Western European and Others Group (WEOG)
Speaker 3: jinhe liu, Civil Society, Asia-Pacific Group
Speaker 4: Jyoti Panday , Civil Society, Asia-Pacific Group
Speaker 5: Jan-Peter Kleinhans, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

1. What is tech nationalism and how widespread is it in the developed and developing world?
2. What cybersecurity threats, if any, are posed by the national origin of 5G infrastructure suppliers?
3. Many observers have detected a subcategory of tech nationalism called "data nationalism" that views

data as a 'national resource' to be 'protected' by the state. What are the arguments for and against this approach?
4. How much of the concern about foreign equipment, software and data use is motivated by economic protectionism and/or national industrial policy rather than cybersecurity?
5. How is it possible to reconcile national cybersecurity with globalized markets for software, services and equipment in the digital economy?
6. Is tech nationalism compatible with multistakeholder governance of the Internet?

Relevance to Theme: The past years have been a turbulent for trade and the digital economy. While protectionist agendas are affecting trade generally, the problem is compounded when national cyber security concerns are linked to trade in digital products and services. This has led to the rise of a phenomenon known as “tech nationalism.” Tech nationalism is a turn away from the globalized supply chains and trading system put in place in the 1990s, and a move toward suspicion and the "othering" of globalized supply chains and foreign producers of software, equipment and services. One of the key drivers of tech nationalism is the ongoing cyber conflict between China and the United States over leadership in 5G technologies. That conflict is militarizing the transition to 5G, cloud and other next-generation Internet technologies.

The question of supply chain security affects a number of Internet-related industries and tends to encourage what some observers have called “alignment” of Internet products and services with national jurisdictions. Some governments have used national security concerns to ban foreign antivirus products and block market access for foreign telecommunication equipment. Some have used cybersecurity rationales for laws that severely restrict outgoing information flows and market access for foreign cloud providers.

Relevance to Internet Governance: National protectionism based on cybersecurity concerns has direct and indirect effects on Internet governance. The Internet helped to globalize the digital economy. A refusal to trust or accept products and services from foreign producers divides the Internet into national walls and limits global connectivity. It also affects the growth of the digital economy. A digital protectionist agenda is not compatible with the argument that the Internet should be governed through a global, multistakeholder mechanism and that it should remain open and interoperable. Moreover, free trade agreements around digital transactions might facilitate the governance of the Internet and its interconnectedness by preventing data localization.

Format:

Debate - Auditorium - 90 Min

Description: The session will discuss the securitization of software and telecom equipment, in the context of the industrial policy competition over 5G, artificial intelligence and other “strategic” technologies that are alleged to be critical to national power. The workshop is presented as a “debate” in that there are two distinct sides to tech nationalism (basically pro and con), but the speakers are not polarized on this and will be able to appreciate the claims of either position. The debate will explore how such securitization affects Internet governance and the digital economy. The panel will include perspectives from the USA, Europe, India, Iran and China, and stakeholders from civil society, private sector and government. It will focus in particular on the battle over 5G infrastructure development but include other arenas such as data nationalism.

Expected Outcomes: The workshop expects to illuminate and clarify the actual nature and scope of the threats provided by 5G infrastructure development.
The workshop is expected to develop a consensus on the best practices needed to reconcile the advantages of globalization and trade with cybersecurity and the mistrust that exists among national governments.
The outcome of the workshop will be summarized and published on the blogs of the organizers, and serve as the building block of additional meetings in the private sector, civil society, and governmental comment periods.

Discussion Facilitation:

The moderator will pose questions and issues to pairs of speakers with contrasting views. They will engage with each other, debating the differences and trying to reach agreement. There will be three rounds of this. Then there will be an opening to the audience to discuss one side or the other. In the final segment the discussion will be steered toward resolution and agreement on best practices.

Online Participation:

Monitor the WebEX chat room and read out the comments
Before the meeting, publicize the link to the room and inform the public that they can attend remotely
Remind various stakeholders and networks that RP is possible and encourage
Work closely with the moderator in person to integrate remote participants in the process

Proposed Additional Tools: Twitter.

SDGs:

GOAL 1: No Poverty
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #44 Building a Bigger Tent: Multistakeholderism and Cyber Norms

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
International Norms
Cyber Security Best Practice

Organizer 1: Government, Western European and Others Group (WEOG)
Organizer 2: Government, Western European and Others Group (WEOG)
Organizer 3: Government, Western European and Others Group (WEOG)

Speaker 1: Kerry-Ann Barrett, Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)
Speaker 2: Paul Meyer, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Sirine Hijal, Government, Western European and Others Group (WEOG)

Policy Question(s):

How can cooperation and collaboration among diverse stakeholders on the national, regional and global levels help to increase cybersecurity and improve national approaches to cybersecurity? How can upcoming 2019-2021 UN processes (OEWG, GGE) on cybersecurity better take into account the perspectives of a broad range of stakeholders with an interest in a secure and stable cyberspace? How can a multistakeholder approach improve national implementation of voluntary cyber norms? And how can this approach foster national cybersecurity policies that advance security, privacy and human rights? What role should different stakeholders play in cybersecurity policy development and capacity building approaches?

Relevance to Theme: Voluntary norms of responsible state behaviour in cyberspace have been developed and agreed multilaterally, notably through UN processes. They remain relevant and continue to be discussed

and further developed in a variety of international settings and fora, including the UN, where two separate processes (the Open Ended Working Group, or OEWG, and Group of Governmental Experts, or GGE) are expected to tackle security and stability in cyberspace in 2019-2020.

Challenges remain in the wide dissemination and implementation of these agreed voluntary norms. For example, many states face challenges in ensuring meaningful stakeholder engagement in the development of their national cybersecurity policies and practices based on these international norms.

The proposed session is meant to focus on how states can better engage with all relevant stakeholders as they seek to implement existing voluntary norms while developing their national cybersecurity policies and practices. It will highlight the perspectives of all concerned stakeholders (civil society, government, academia, private sector) and how they can be engaged in these national processes. It is also an opportunity for IGF participants to discuss how upcoming 2019-2021 UN processes on cybersecurity can better take into account the perspectives of a broad range of stakeholders with an interest in a secure and stable cyberspace.

Relevance to Internet Governance: The session focuses on how governments, the private sector and civil society, in their respective roles, can work together in implement agreed norms of responsible state behaviour at the national level in ways that lead to the development and growth of an open, free, secure and stable cyberspace.

Format:

Panel - Auditorium - 90 Min

Description: Moderator will introduce the topic with a five-minute historical recap of the voluntary norms of peacetime behaviour developed by the 2013 and 2015 UN Group of Governmental Experts on ICTs and endorsed by the UN General Assembly; and then highlight the major challenges to address:
- How to advance the implementation of existing international norms at the national level.
- How to ensure broad stakeholder engagement in the development of national cybersecurity policies and practices stemming from these international norms.
Six speakers will be asked to provide short (approximately 5 minutes) presentations on their perspectives on the two issues identified above. These speakers would be:
- A Canadian government representative: Sirine Hijal, Canada's deputy cyber foreign policy coordinator
- A representative from civil society: Paul Meyer from ICT4Peace
- A representative from academia/think tank: TBC
- A representative from the private sector: TBC
- A government representative from a developing country: TBC
- A representative from a regional organization: Kerry-Ann Barrett from the Organization of American States

The moderator will then ask panelists questions in turn to stimulate debate and dialogue, particularly where there are opposing views on the way forward. The audience will also be provided with the opportunity to ask questions and intervene to further enhance the debate.

Expected Outcomes: - Greater awareness among participants of existing voluntary international norms and challenges to their implementation.
- Increased awareness among participants of the importance of multistakeholderism for the development of national cybersecurity policies and practices.
- Concrete proposal for enhancing multistakeholderism in the development of national cybersecurity policies and practices.
- Concrete proposals for enhancing consultations in the upcoming UN-based OEWG and GGE processes, which the organisers will relay in their national contributions to these UN processes.

Discussion Facilitation:

The moderator will directly engage with the audience (including online) by encouraging them to ask questions and intervene to further enhance the debate. Half the session duration have been set aside for

interaction with the audience.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #45 Democracy and Civic Engagement in a Digital Society

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Civic Engagement online
Fake News
FoE online

Organizer 1: Technical Community, African Group
Organizer 2: Private Sector, African Group

Speaker 1: Marianne Elliott, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Menno Ettema, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 3: Johannes Baldauf, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Mira Milosevic, Civil Society, Western European and Others Group (WEOG)
Speaker 5: Jasmin Mittag, Civil Society, Western European and Others Group (WEOG)
Speaker 6: Hannes Ley, Civil Society, Western European and Others Group (WEOG)
Speaker 7: Matthew Rantanen, Technical Community, Western European and Others Group (WEOG)
Speaker 8: Nadia Tjahja, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

How have civic engagement and social commitment changed under the influence of digitisation of society? How does government encourage, support and acknowledge civic engagement, how relates this to corporate social responsibility from the private sector, and what role does the Internet play in this regard? Do we need common rules and standards for civic engagement online and who will set them? Top-down or bottom-up: how does government support counter narrative strategies, what impact does that have compared to alternative narratives as an output of civic engagement?

Relevance to Theme: Civic engagement and social commitment are two pillars of society both having the potential to contribute to a healthy and safe digital environment when performed in and with social media. By civic engagement online new communities are built and already existing communities are strengthened. Thus online engagement supports the stability of society at large as well as the stability of smaller communities. On the other hand fake news and narratives based on false information are threatening society and have the potential to eradicate democratic values. While it is important to ensure human rights such as freedom of expression and access to information it is also necessary to provide measures for the safety of users worldwide in order to empower them to cope with such threats. Only a balanced approach will help us to achieve stability and resilience of the digital society in the future.

Relevance to Internet Governance: As laid down before it needs joint efforts from all stakeholder groups to ensure that common rules and standards for civic engagement in and with social media are set and adhered

to. Internet Governance provides for a framework in which such common rules can be developed and brought into acceptance by joint efforts of governments, private sector, academia and civil society. Since phenomena such as hate speech, fake news and challenges to electoral integrity are not bound by borders Internet Governance needs to address these issues on a global level. Therefore it is of paramount importance to bring forward this debate to the global IGF, deploy experiences of best practice examples from around the world and thus initiate decision-making in order to cope with the challenges that lie ahead of us.

Format:

Round Table - U-shape - 90 Min

Description: In reference to SDG 16 peaceful and inclusive societies build the basis for promoting democratic values, social commitment, civic engagement and political participation. However, in an ever more digital society, democratic values are threatened by hate speech, fake news, challenges to electoral integrity, etc. Stability and resilience are not only an issue of (technical) infrastructure, these terms must also be understood in regard of a stable and resilient society. Democracy has come under pressure and this is in a way amplified by digital, social media. But certainly social media can help counteract these threats, and social media can also be used to promote civic engagement, social commitment and participation, having the potential to prevent threats from developing in the first place. A recently carried out study based on about 620 examples of civic engagement in and with social media has given evidence of the interrelationship and the effects of social media for social good (please refer to background paper). In the workshop, we will bring together stakeholders from various backgrounds in order to discuss which part governments, civil society, and the private sector can and must play to ensure stability of a digital and democratic society.

Expected Outcomes: The workshop attempts to achieve the following outcomes
- Highlighting and comparison of experiences from diverse best practice examples of civic engagement and social commitment as a basis for common rules and standards
- Lessons learned on scalability and transferability of social media strategies for social good
- Conclusions on the impact government strategies can unfold
- An outline for common rules and an answer to the question what role self-regulation can play in this regard

Discussion Facilitation:

Firstly the scene will be set and each of the four speakers will contribute from their specific stakeholder perspective as researchers, government and private sector representatives. Then the floor will be opened and representatives from diverse communities will show-case their examples of civic engagement. Since we apply for a roundtable session these best practices will facilitate the discussion with participants in the room and online.
The co-organisers and co-moderators both have a legal background and will therefore be able to steer the debate towards fruitful outcomes in regard of the policy questions relevant to the theme of the workshop.

Online Participation:

The Policy Questions and an outline of the session will be sent in advance to the communities of organiser and co-organisers, the speakers and best practice representatives. Thus we expect to have several hundred people informed about the session. They will be invited to bring their comments and questions forward either in advance of the session or by online participation. The online moderator will monitor contributions from online participants throughout the whole session, he will invite online contributions especially after each of the four speakers and also after the presentation of best practices.
The community network members will also use their social network contacts to spread the message and outcomes further after the session.

Proposed Additional Tools: Organiser, Co-organisers and best practice representatives will make use of their social media channels to inform their communities on the session and the issues that will be addressed.

SDGs:

GOAL 5: Gender Equality
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

IGF 2019 WS #54 Public and private definition of content standards and FOE

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Fake News
FoE online

Organizer 1: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Chinmayi Arun, Civil Society, Asia-Pacific Group
Speaker 2: David Kaye, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 3: Emma Llanso, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

- What are the main elements in the debate about legal and/or regulatory frameworks for the definition and application of content standards by online platforms?
- How freedom of expression principles can be applied to an environment that combines public and private rules?
- What are the current practices and tendencies regarding the regulation of content standards by States or supranational bodies like the EU?
- Which are the best venues for dialogue and cooperation between platforms, civil society, and public authorities in this area?

Relevance to Theme: The debate about how platforms define and apply their content rules and the implications in the area of liability is nowadays at the center of many Internet policy debates. The growing concern about the presence and availability of hate speech, fake news, terrorist content and other illegal and harmful items on online platforms is directly linked to the emergence of regulatory proposals to reinforce trust and accountability in the online world. This theme also reflects the tension between the alleged need to better regulate the responsibilities and the role of platforms vis-a-vis content on the one hand, and the need to avoid creating new and indirect forms to restrict the exercise of the right to freedom of expression when such right is excercised through private online distribution platforms, on the other hand.

Relevance to Internet Governance: The proposed topic is of central importance in the current process of defining the rules framing online content distributed via platforms. The objective of the session is precisely to discuss the best possible way to define such norms as the result as a combined effort and dialogue between platforms, governments, media, and civil society.

Format:
Debate - Classroom - 90 Min

Description: The session will be structured as follows:

a) General introduction by moderator.
b) Intervention by David A. Kaye, UN Rapporteur on Freedom of Opinion and Freedom of Expression. This intervention will describe the applicable international standards and the documents adopted by international and regional organisations on the issues related to the theme of the session.
b) Intervention of Emma Llanso, from Center for Democracy and Technology. This intervention will describe the effort made by civil society in different parts of the world, in dialogue with governments and online companies, to find a correct balance between the responsibilities of online platforms, the competences of governments in areas like fake news, hate speech or online terrorist content, and the need to protect freedom of expression as a fundamental principle.
c) Chinmayi Arun, from National Law University Delhi will describe some practices and problems related to this area in countries of the global South, as well as the way solutions adopted in Europe and The United States may have a special influence in other regions of the world.

After these presentations, participants in the audience will be asked to share and discuss specific cases, experiences and approaches. The panel aims at fostering a debate that shall combine a human rights and international standards approach together with a proper consideration of the adequate tools to effectively deal with illegal and harmful content.

The debate will also identify particular global and regional tendencies aiming at transforming the general liability system applicable to online platforms, as well as possible actions and efforts to properly tackle these tendencies and adequately understand the impact on freedom of expression."

Expected Outcomes: - Enable and encourage civil society organizations to pay particular attention to new legislative proposals in any regions of the world regarding online content moderation, and properly assess their impact on freedom of expression.

- Increase the number of advocacy and sensitization activities regarding the role of online platforms as facilitators of the exercise of the right to freedom of expression, and the impact that certain legal provisions can have on them.

- Increase the awareness among main stakeholders (civil society, international organizations, etc.) on the ongoing debates about the combination of public and private rules for the establishment of content standards, as well as on the need to engage and collaborate in the adoption of a proportionate and adequate model.

Discussion Facilitation:

Initial presentations will be brief and basically present main ideas and suggestions on the topic. Participants will be asked not only to interact and discuss with speakers but also to assist in the formulation of policy proposals and specific actions applicable to ongoing cases and discussions in different areas of the world.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: The session will have a hashtag to promote engagement via Twitter from interested participants not present in the event.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #59 Digital Sovereignty and Internet Fragmentation

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
FoE online
Trust and Accountability

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Eastern European Group
Organizer 4: Civil Society, Western European and Others Group (WEOG)
Organizer 5: Civil Society, Western European and Others Group (WEOG)
Organizer 6: Civil Society, African Group
Organizer 7: Government, Latin American and Caribbean Group (GRULAC)

Speaker 1: Mona Badran, Civil Society, African Group
Speaker 2: Alexander Isavnin, Technical Community, Eastern European Group
Speaker 3: Peixi XU, Civil Society, Asia-Pacific Group
Speaker 4: Achilles Zaluar, Government, Latin American and Caribbean Group (GRULAC)
Speaker 5: Vint Cerf, Private Sector, Western European and Others Group (WEOG)
Speaker 6: Lise Fuhr, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

The policy questions can be classified into three headings:

1. The nature of national sovereignty and its extension to 'digital sovereignty' or ‘cyberspace sovereignty’
- Is digital sovereignty compatible with the globalized access provided by the Internet protocols? What is gained and what is lost by trying to make cyberspace conform to principles of territorial sovereignty?
- How does sovereignty in cyberspace relate to/differ from traditional notions of sovereignty that shaped international communications policy since the 1850s?
- Why and how are countries trying to create "national Internets?" Are these efforts compatible with a global internet or will they lead to fragmentation of the infrastructure or the services and processes that it supports?

2. National and global effects of digital sovereignty:
- How do attempts by some countries to create a "sovereign Internet" affect the human rights of Internet users?
- How do national boundaries on data flows affect economic development, competition and efficiency in the global digital economy?
- How does sovereignty in cyberspace affect the security and privacy of Internet users?
- How do they impact foreign firms seeking to operate locally? Are they consistent with international trade and other multilateral obligations?

3. Governance responses:
- Would it be better to conceive of cyberspace as a global commons similar to the high seas or outer space? What are the policy and governance implications of classifying cyberspace as a global commons?
- What blend of institutional settings would be useful in addressing the conflicts engendered by by strongly statist digital sovereignty practices? What would be the role of e.g. security arrangements, international trade agreements, international privacy agreements, MLATs and other efforts to deal with access issues of concern to law enforcement and others?
- Is there any role in this discussion for multistakeholder cooperation, or is sovereignty a matter on which only states should engage? If there is a role, how could this be structured?

Relevance to Theme: The problem of how to achieve security, stability, safety and resilience needs to be discussed in the context of understanding the role of sovereignty in cyberspace. National sovereignty is the organizing principle of the traditional international political system. In the traditional sovereign model, national governments take most of the responsibility for protecting security, stability, safety and resilience. But because sovereignty is bounded by territory, their authority stops at their borders. The Internet, in contrast, is transnational in scope and provides the potential for borderless connectivity. Thus in cybersecurity traditional security and stability practices have had to be modified, often relying on multistakeholder cooperation and cross-border operations in which the power of states is shared with many other actors.

Today, in a context of cyber-attacks by state actors and a globalized digital economy, efforts to assert territorial control into cyberspace and project it onto all things digital are gathering momentum. Across the world, governments of many political complexions are considering or have adopted broad policy frameworks they say are necessary to maintain what they variously describe as cyber, data, informational, digital, or technological sovereignty. They have been implemented via such measures as forced data localization, barriers to cross-border data flows, routing and surveillance requirements, digital industrial policies and trade protectionism, and censorship and blocking of classes of data flows or Internet-based platforms. Russia and China are prime examples but many other countries are assessing these different models.

This roundtable includes participants from Russia, China, Brazil and Argentina as well as Iran, the USA and Europe.

Relevance to Internet Governance: The tension between national sovereignty and the global Internet is probably the single most fundamental Internet governance issue today. The Internet protocols create a globally connected virtual space in which anyone from anywhere in the world can communicate; in the technical structure of cyberspace distance and territory do not matter. Governmental authority, on the other hand, is bounded by geographic territory and each government is supposed to have supreme authority in its territory. Ever since the World Summit on the Information Society, governments have been trying to insert the concept of sovereignty into Internet governance discussions. On the other hand, many Internet users, platforms and service providers have been promoting the benefits of seamless global interconnection. There is a clash between the two distinct models of Internet governance. The tension between sovereignty and globalization plays out in several Internet governance issues. The debate over data localization often appeals to “technological sovereignty.” The global debate over cybersecurity and cyber norms also has struggled to understand how notions of sovereignty can be reconciled with the globalized espionage and attack capabilities provided by cyberspace.

Format:

Round Table - Circle - 90 Min

Description: The purpose of this workshop is to explore the new discourse and practice of national sovereignty over cyberspace and to consider its implications for Internet openness vs. fragmentation. The session would be organized as an interactive roundtable. In the first half, the moderators would pose a few policy relevant questions pre-arranged with speakers and foster fluid debate. In the second half the floor would be opened to dialogue with all in-person and remote participants.

The roundtable has a highly diverse set of organizers and a well qualified set of discussants. The people and organizations proposing this workshop are from Europe, Iran, Egypt, USA, Argentina and Russia. It will be moderated by Milton Mueller and William J Drake, prominent academics who have written seminal scholarly works on the topics of cyberspace sovereignty and Internet fragmentation. Discussants include Lise Fuhr, the Danish director of the European Telecommunications Network Operators Association. Vinton Cerf of Google is one of the founders of the Internet and a key figure in the Internet technical community. Two perspectives from Russia are included. Co-organizer Ilona Stadnik is an international relations scholar from St. Petersburg University, Russia. Alexander Isvarin heads the Internet Protection Society of Russia, a civil society organization that advocates for Internet freedom in the country. Ambassador Achilles Emilio Zaluar Neto, from the Foreign Ministry of Brazil, is a government stakeholder. Xu Peixi, Communications University

of China, is a leading Internet governance scholar from China. Mona Badran, Cairo University Egypt, specializes in the study of digital trade.

Expected Outcomes: The workshop will produce a better understanding of the technical and economic feasibility of the various digital sovereignty models being considered or implemented around the world and their implications for global Internet governance. The workshop is expected to clarify what is really happening and dispel any myths about cyber-sovereignty proposals. The workshop is expected to foster a more informed dialogue between the BRIC nations and Internet globalization advocates about governance models for cyberspace.
The organizers of the roundtable have specific plans for disseminating the ideas and outcomes from this panel into other forums and to the public. They will develop a report on the workshop outcomes and publish it on their widely-read websites. Results will be taken into cybersecurity conferences such as CyCon in Tallinn and Cycon US. Internet institutions such as ICANN, regional Internet registries and IETF are also forums for continuing the discussion of this problem.

Discussion Facilitation:

The roundtable format will allow a dynamic and flexible discussion. The moderators are experienced Internet governance scholars and participants who understand the different points of view. The group of organizers have 13 years of experience in organizing and facilitating IGF workshops and Schools of Internet Governance in different world regions. They will allow the contrasting views and national perspectives to be presented at the outset and then open it up to reactions and responses from the other roundtable participants. At least 30 minutes of the 90 minutes will be reserved for audience and remote participant questions and comments. It should be noted that Internet Governance Project, which is rooted in academia, has organized dozens of successful roundtables and panels both inside and outside of IGF and is very experienced at managing them.

Online Participation:

We will use it to allow remote participants to submit questions or directly participate in the discussion in real time.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #60 Cyber-Accountability: Building Attribution Capability

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Brenden Kuerbis, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Farzaneh Badii, Civil Society, Asia-Pacific Group
Speaker 3: Serge Droz, Private Sector, Western European and Others Group (WEOG)
Speaker 4: jacqueline eggenschwiler, Technical Community, Eastern European Group

Policy Question(s):

Attribution is defined as identifying with an understood degree of confidence who is responsible for a cyber-attack. It is important, particularly in view of emerging norms for responsible state-behavior in cyber space, because it contributes to the accountability of actors in cyberspace. Our proposal addresses the following policy questions:
1. What is wrong with how cyber-attributions are conducted today?
2. How can we make the cyber-attribution process more objective, scientific, transparent and widely accepted?
3. Will making neutral, accurate and authoritative cyber-attributions improve accountability and help reduce cyber-attacks?

Relevance to Theme: In the last decade, state actors have become one of the most important sources of cyber-attacks because such attacks serve their foreign policy, military or espionage goals. These attacks tend to generate retaliation and a cyber “arms race” among other state actors and may create large collateral damage beyond the intended target. This kind of escalation and conflict threatens the security, stability, safety, trust and resilience of the Internet.
Although states claim to be working on cyber norms that would reduce these activities, we cannot enforce international cyber-norms unless we can hold actors who violate them responsible. Holding cyber-attackers responsible for their attacks requires "attribution" - that is, accurate identification of the perpetrator. But governments and their cyber-armies are usually unwilling to conduct or accept neutral and scientific attributions. Their decision to publicly attribute depends on the political stakes, and behavior can be strategic and even deceitful. Successful attribution involves credibly explaining a finding and the evidence basis to the public in a reproducible manner. But states’ attribution claims are often based on intelligence that they are not willing to publicly share, which raises persistent questions about how their findings were reached and whether they are true.
This workshop will explore ways that civil society and business can work together to institutionalize the cyber attribution process, and put it in the hands of credible non-state actors who are not parties to inter-state conflicts.

Relevance to Internet Governance: Cybersecurity is one of the most important domains of Internet governance. The security, stability, safety and resilience of the Internet will be improved it we can develop new institutions and processes to conduct credible cyber-attributions. Attribution contributes to governance by fostering accountability.

Format:
Break-out Group Discussions - Round Tables - 60 Min

Description: The session will inform participants about an ongoing effort to form a global network of cybersecurity researchers who want to cooperate to develop attribution capabilities, and perform cyber-attributions of state-sponsored cyber attacks. The goal is to perform attributions that are considered scientific and credible by the community. Attribution is defined as identifying with an understood degree of confidence who is responsible for a cyberattack. It is important because it contributes to the accountability of actors in cyberspace. Accountability for cyber attacks has increasing geopolitical significance. Attribution made by one nation-state is unlikely to be accepted as neutral and authoritative by other nation-states, especially if those states are rivals or hostile. Various commentators on this issue have proposed that a transnational attribution organization exclude governments and be led by experts in academia and business. The Internet Governance Project (IGP), ICT4Peace, and several other organizations are forming the nucleus of an informal network of universities and civil society organizations who want to become involved in cyber-attribution and attribution research.

As a breakout group discussion, this session does not really have "speakers;" it is organized as an informational and discussion session amongst any researchers and businesses who are engaged in or interested in cyber-attribution. However, discussion will be led and moderated by 4 people who attended the Toronto workshop forming the network. They will update the group on the formation of the network and facilitate engagement of new people and organizations.

Expected Outcomes: The main expected outcome is to identify additional participants who want to contribute to a research network on attribution.
Another outcome is to improve understanding of the challenges of conducting globally credible cyber-attributions

Discussion Facilitation:

This is an interactive session. Attendees in the room and remote participants will have the chance to interrupt and make comments at any time during the discussion.

Online Participation:

The official online tool will allow remote IGF participants to send in questions. For more robust discussion we will use the Blue Jeans video link described below

Proposed Additional Tools: We will also set up a BlueJeans room at Georgia Tech. Blue Jeans is a remote participation tool with improved video and audio capabilities that will allow students and youth to attend the sessions remotely.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #63 Usual Suspects: Questioning the Cybernorm-making Boundaries

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Cyber Security Best Practice
Internet Protocols

Organizer 1: Technical Community, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Sumon Ahmed Sabir, Technical Community, Asia-Pacific Group
Speaker 2: Mariko Kobayashi, Private Sector, Asia-Pacific Group
Speaker 3: Louise Marie Hurel, Civil Society, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

Cybernorms Development Processes have been different in how they reach agreement; how committed they are in implementing these norms; how open they are in including different stakeholders in their discussion

and their adoption; how they account for technical consequences or mediate between political motivations. What can we learn from these processes? Which ones have been more successful? Is there scope for optimism in improving these processes for them to be more effective? More inclusive? More representative? More technically feasible? More impactful in improving cooperation on cybersecurity?

Relevance to Theme: Several groups, bodies, and organizations have been involved in developing "Cybernorms" as an answer to cybersecurity needs and promoting responsible State behavior in cyberspace. Most formally, there is the UN Group of Governmental Experts (UNGGE). But there are other initiatives that are fostering cooperation on cybersecurity: most recently G7 Dindard Declaration, the "Paris Call for Trust and Cybersecurity in Cyberspace" and the ongoing work of the "Global Commission on the Stability of Cyberspace". At the regional level, different organizations have been discussing "Cybernorms" as well: ASEAN, OSCE, OAS, AU, SCO, NATO, EU, etc. Despite the best efforts of all these groups, bodies and organisations, there has been little progress for these "Cybernorms" to have meaningful impact in improving cybersecurity. This is most true in the political domain. Be it the failure of the GGE or the emergence of two-track processes (GGE and OEWG), such developments have played a key role in resurfacing fundamental questions related to the implementation and objective of these Cybernorms. Meanwhile, in the technical domain, we observe a range of widely accepted norms, but not well known or understood in the political arena. These are widely acknowledged, agreed principles, practices and behaviours (or restraint from behaviors), such as MANRS, RIR policies, the IETF Best Current Practices, etc., efforts that have guided cybersecurity efforts and have had positive impact throughout the years. It is important, then, to discuss what is the appropriate role of the technical community in contributing to the Cybernorms Development Process. How to foster Cybernorms effectiveness, by eliciting an expectation of justification by States if meddling with technical norms. Whether multilateral norms making is better (or more likely to be effective) vs. other areas where norms for industry are more needed, and, of course, which areas most need multistakeholder processes (and which don't).

Relevance to Internet Governance: This roundtable will be the fourth in a series of efforts at the IGF to bring the global policy and technical communities into closer and more effective dialogue. By focusing on technical perspectives on "Cybernorms", we may be able to move the dial on stalled debates and, at the same time, we may develop useful insights into the inherent problems with the processes and mechanisms that have been leaned on to develop "Cybernorms" thus far. In our first workshop in 2016, "NetGov, please meet Cybernorms. Opening the debate", participants agreed that there are many elements in the Internet Governance history and processes worth considering when developing "Cybernorms". In our second workshop in 2017, "International Cooperation Between CERTS: Technical Diplomacy for Cybersecurity", we explored the importance and the value of the technical community's involvement in international discussions on cybersecurity. In our third workshop in 2018, "Whois Collected, Disclosed and Protected: CERTs Viewpoint" we deepened the discussion into an example of how State led regulatory efforts can have unintended consequences affecting cybersecurity cooperative efforts. We have strong foundations to argue that the Cybernorms Development Processes are and should be intrinsically related to Internet Governance debates and the former could greatly benefit by exploring best practices on more open and inclusive processes -- that is, including the views of the technical community. Moreover, the 2019 edition of the Best Practice Forum on Cybersecurity is currently working on exploring best practices in different Cybersecurity Initiatives and the implementation of suggested measures. Our workshop is relevant and complements the work of the BPF on Cybersecurity.

Format:

Round Table - Circle - 60 Min

Description: SETTING THE SCENE. 15 mins. This session will depart from a sequence of thought-provoking questions: (i) What do we understand by "Cybernorms"?; (ii) What sort of "Cybernorms" can be more effective in improving cooperation, whether in the technical arena or between States?. DISCUSSION. 20 mins. A facilitated discussion will deepen on the questions at hand: (i) What are the key characteristics (or best practices) guiding effective Cybernorms development processes; (ii) How do they differ when confronting different cybersecurity solutions? In particular, we will ask (iii). Whether more open and inclusive processes would deliver more meaningful "Cybernorms". PEAK. 10 mins. An open discussion will occur between

participants: (i) Why there has been little progress of UNGGE "Cybernorms" to have meaningful impact in improving cybersecurity? (ii) What is the appropriate role of the technical community in contributing to the Cybernorms Development Process. CONCLUSION. 15 mins. How to foster Cybernorms effectiveness? Whether multilateral norms making is better (or more likely to be effective) vs. other areas where norms for industry are more needed? Which areas most need multistakeholder processes (and which don't)?

Expected Outcomes: Analyzing Cybernorms development as an Internet Governance process offers a new approach which has the potential to: 1. Offer practical solutions to solve the political impasse on the production of new Cybernorms. 2. Offer an appropriate and inclusive channel for the technical community to participate in the early stages of Cybernorms development, offering risk assessment and feasibility analysis for Cybernorms agreements, and practical steps for Cybernorms implementation. 3. Offer fresh ideas on what could constitute best practice in Cybernorm Development Processes.

Discussion Facilitation:

There are three key ingredients that have proved a successful recipe in the previous 3 IGF workshops that we have organized: strong moderation, fast pace interactions and diverse points of view. We have had an initial core team, which includes the organizers and an initial set of speakers (which are included below). As the attendants to the IGF are confirmed, we expand this core group adding other experts as speakers. This is the reason why we keep a round table as a desired format (and not a panel): the idea is that in a short time space, there will be as many points of view being put on the table. The art of the workshop relies in the capacity of the moderators to thread these views carefully, firstly, into an intense debate, secondly, into a fresh set of agreed conclusions, which will effectively take the discussion few steps further. We will juxtapose speakers from Academia, Government, Private Sector, Technical Community, Civil Society and Youth and then build possible tracks for agreement until we conclude with a list of innovative solutions for the questions at hand.

Online Participation:

We will be promoting the workshop widely, not only to IGF registered participants, but also for people to follow it live through online channels. We will be using social media as additional channels for participation. In spite of technical challenges, we have successfully added voices from remote participants to our sessions. Via live video, just audio and also channeling questions and views through interventions via the chat boxes. We encourage remote participation.

Proposed Additional Tools: Maybe. We are open to use survey apps or other tools to facilitate the discussion.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #85 Misinformation, Trust & Platform Responsibility

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
FoE online
Trust and Accountability

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Technical Community, African Group
Organizer 3: Civil Society, Asia-Pacific Group

Speaker 1: Minna Horowitz, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Arthur Gwagwa, Technical Community, African Group
Speaker 3: Ansgar Koene, Civil Society, Western European and Others Group (WEOG)
Speaker 4: shu wang, Private Sector, Asia-Pacific Group
Speaker 5: Jinjing Xia, Private Sector, Asia-Pacific Group

Policy Question(s):

What are the reasons for the proliferation of disinformation and fake news in different countries and regions?
What are the mechanisms used in disinformation and fake news mitigation? And How effectiveness are they?
What role should technology (e.g algorithm) play in disinformation and fake news refutation?
What roles should Internet platform play in disinformation and fake news refutation? What kind of collaboration could be created among Internet platforms and media outlets to fight disinformation and fake news?
What are the best practices in terms of disinformation and fake news refutation in light of freedom of speech and the necessary neutrality and legal certainty for platforms?
How can trust and accountability to the internet platforms and government interventions be restored?

Relevance to Theme: The IGF community is considering the potential risks to the security and stability to the Internet, and how to achieve the safety and resilience of a healthy digital environment. The session will contribute to the discussions of fake news, trust, accountability, and freedom of expression under the theme "security, safety, stability and resilience". It will address those issues by looking at online disinformation and fake news refutation from different stakeholders' perspectives. Specifically, the workshop will discuss: 1) the responsibilities of Internet Platforms and government regulators in fighting the online fake news and disinformation; 2) the role of technology (such as AI & Algorithm) in fake news and disinformation refutations; 3) how to hold Internet platforms and government accountable; 5) How to restore the public trust in the Internet Platforms, government, and the news media; 6) How can globally accepted standards and best practice be developed. The topics of discussions make this panel directly relevant to the theme "security, safety, stability and resilience."

Relevance to Internet Governance: The proposed session will discuss the timely issues of fake news and disinformation, information security and online safety, responsibility and accountability of digital platforms, and function of government regulation and trust in platform and government in the Internet governance. It will involve stakeholders from the private sector, civil society, and technical sectors at both developed regions (EU and US) and developing regions (China and Africa) to share their professional knowledge, experiences, best practices, policy framework in disinformation and fake news refutation. The proposed session will facilitate the global debate as well as shaping the evolution of norms, principles, best practices of online disinformation and fake news mitigation and model of Internet governance.

Format:
Panel - Auditorium - 90 Min

Description: The creation, dissemination and accumulation of information is one dimension of structural power. The vast majority of conflicts today are not fought by nation states and their armies; increasingly, they are fought not with conventional weapons but with words. A specific sort of weaponry—"fake news" and viral disinformation online—has been at the center of policy discussions, public debates, and academic analyses in recent years (Horowitz, 2019). Technology, including digital platforms, that enable connections and participation can be used for misinformation and fake news. In addition, what has been called the

“emerging information arms race” (Posetti & Matthews, 2018, July 23) is plaguing mature and emerging democracies alike (Horowitz, 2019). A variety of approaches has adopted in different regions/localities to flight disinformation and fake news from content intervention (fact-checking and filtering), technical intervention (dedicated anti-rumor platforms, algorithm) to economic intervention (undermining advertising sources)， legal intervention (civil and criminal penalties) and etc. Different stakeholders including state actors, NGOs, platforms, news media are involved. However,
How effective are those approaches, what are the shared policy principles, norms and mechanisms?
What are the responsibilities of actors such as Internet platforms and government regulators?
What roles do technology (e.g. algorithm and bots) play in the process?
How can we hold the actors accountable for their interventions?
How can we encourage cross-region and cross-sectors collaborations?
What are the best practices in light of freedom of speech and the necessary neutrality and legal certainty for platforms?
How can we restore the trust of the public to the Internet platforms, news media and politics?

In this session, speakers and moderators from China, UK, Finland, Africa will discuss the above questions from diverse geographic and stakeholder’s perspectives.

Dr. Minna Horowitz, Docent professorship at the University of Helsinki; Expert, Digital Rights and Advocacy, Central European University, Center for Media, Data, and Society

Dr. Ansgar Koene, Chair of IEEE P7003 Standard for Algorithmic Bias Considerations working group; Senior Research Fellow, University of Nottingham, HORIZON Digital Economy

Ms. Jingjing Xia, The Bytedance Techkind Center, BYTEDANCE TECHNOLOGY CO, China.

Mr. Shu Wang, Deputy Editor, Sina Weibo, China

Mr. Arthur Gwagwa, Centre for Intellectual Property and ICT Law: Strathmore Law School, Kenya

Onsite Moderator: Dr. Yik Chan Chin, Xi’an Jiaotong Liverpool University
Online Moderator: Mr. Jinhe Liu, Tsinghua University

Intended Panel Agenda:

Setting the scene: onsite moderator, Dr. Chin, 5 minutes

Four presentations, each speaks for 9 minutes with 1 minute of immediate audience response
1) Minna Horowitz
2) Shu Wang
3) Ansgar Koene
4) Jingjing Xia
5) Arthur Gwagwa

Discussions amongst speakers 10 minutes, moderated by Dr. Chin

Interactive question and answer session, 30 minutes moderated by Dr. Chin and Mr. Liu.

the wrap-up of the moderator, 5 minutes

Expected Outcomes: 1) Facilitate the debate as well as shaping the evolution of norms, principles, best practices of online disinformation and fake news refutation and model of Internet governance.
2) Identify differing viewpoints regarding Internet governance approaches regarding AI to help the creation of an environment in which all stakeholders are able to prosper and thrive
3) Policy recommendations and key messages report to the IGF community
4) A collaboration amongst speakers who are from different stakeholder sectors, in fake news and disinformation refutation and researches.

Discussion Facilitation:

The session will be opened by the onsite moderator to provide participants an overview of the topics discussed in the session, the professional background of the speakers, and the format of interaction. Each speaker will give short presentations providing basic knowledge to the audience of their topics. The moderator will ensure the audience from both offline and online being able to ask questions to the speakers immediately following their presentations to encourage active participation. In the third part, the session will move to the discussions and debate. The moderator will invite each speaker to express their views on a set of questions and guide the debate amongst speakers and the audience to foreground their common ground and differences. The workshop organizers and moderators will discuss the content of questions with speakers in advance to ensure the quality and flow of the discussion and debate. In the third part, moderators will invite questions from the audience and online participants, the question time will last about 30 minutes in order to provide sufficient interactions amongst speakers, audience and online participants. Online participants will be given priority to speak, and their participation will be encouraged by moderators. The onsite moderator will summarise the findings and recommendations and future actions of the panel.

Online Participation:

The online moderator will participate in the online training course for the Official Online Participation Platform provided by the IGF Secretariat's technical team to ensure the online participation tool will be properly and smoothly used during the proposed session.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #92 Public Health Online: Shadow Regulation-Access to Medicines

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Human Rights
Internet ethics

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Oki Olufuye, Government, African Group
Speaker 2: Jillian Kohler, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 3: Aria Ahmad, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

Innovation and consumer choice are at the heart of the internet. In an increasingly globalized digital marketplace, however, there is a growing need to develop standards that protect the health and safety of consumers. The sale of medicines over the internet represent one of the fastest growing markets, driven largely by a lack of affordability and domestic availability. According to the World Health Organization

(WHO), over two billion people lack regular access to essential medicines. Meanwhile, hundreds of millions of people have used the internet to fill legitimate prescriptions from both domestic and foreign pharmacies.

While consumers increasingly turn to internet pharmacies, there is a critical gap in guiding principles or standards that apply across national boundaries. Instead, we have a legislative and regulatory patchwork with uneven jurisdictional coverage, frequently outdated, and enforced disproportionately. The lack of transnational principles, guidelines and/or standards as they apply to internet pharmacies has at least two implications to consumer choice and consumer safety. On the one hand, it undermines access to affordable and quality medical products from legitimate internet pharmacies, while simultaneously failing to address the risks posed by rogue actors that sell falsified or substandard medical products, often without a valid prescription. In order to fend off the growing public health moral hazard, there is a fundamental need to develop appropriate international regulatory guidelines. Every day, people all around the world use the internet to purchase products and services wherever they find them at a price they are prepared to pay, for a legitimate product. Pharmacy is no different. What is required, in other words, are 'digital' standards to augment outdated 'analog' laws.

The aim of this Workshop will be to examine a practical and pressing case study of digital governance as it applies to a growing public health need. While the initiative may be novel in the context of an IGF event, it builds on years of work that culminated in 2018 with the adoption of the Brussels Principles on the Sale of Medicines Over the Internet ('Brussels Principles', www.BrusselsPrinciples.org) developed by a coalition of stakeholders, internet experts and civil society at RightsCon Brussels 2017 and Toronto 2018. For the IGF Workshop, however, we hope to convene a unique group of stakeholders to take up the outstanding technical and policy challenges while imagining the future of digital governance of transnational internet pharmacies.

Participants at the Workshop will range across Governments, internet policy experts, professional associations, academia, civil society, the private sector, certification agencies, and online pharmacies. The objective will be to present the first multi-stakeholder-developed set of standards to meet appropriate legal and regulatory regimes, industry and consumer needs, while applying an approach that provides practical tools to address an increasingly global healthcare crisis.

Building on the Brussels Principles, the IGF Workshop will attempt to address the following set of policy and technical questions:
1. How do we move beyond the Brussels Principles to adopting guidelines and/or standards that apply to transnational internet pharmacies which protect consumer choice but also patient safety? What are the outstanding technical internet governance and policy challenges?
2. Countries have differing regulatory models for approving and marketing medicines within national markets: can a global standard be advanced through a multi-stakeholder approach that applies to physical and online pharmacies?
3. Medical professionals are accredited nationally – how can a regional and/or global accreditation system work for online medicine dispensing? Who would undertake the accrediting?
4. Regulators are also often limited to working within national systems – is it possible to achieve a different accreditation system? What organization could oversee such a regulatory accreditation system, e.g. the World Health Organization?
5. Is a treaty needed? Given how slow and resource intensive treaty development can be, would it be possible to envision standards and multi-lateral agreements in providing the needed "governance" for online pharmacies – identifying standards for practice and oversight? Is there a possible model which could be examined, e.g. the World Intellectual Property Organization Patent Treaty?

This Workshop will concentrate on legislative and internet policy challenges, while presenting the first and only multi-stakeholder-developed set of standards to move the dialogue forward with appropriate legal regimes, industry and consumer's needs.

Relevance to Theme: In the increasingly digitized world, as we work to achieve the UN's Sustainable Development Goals that affect how quality healthcare affects all citizens, especially in resource-limited settings, safe and secure interactions online are of primary importance. High prices for medicines present a

growing global health challenge to countries of all income levels, including higher-, middle- and low-income, both in developed and developing countries.

In his address at the 2018 IGF Paris, the UN Secretary General stated that the digitization of the world affects all citizens, and both daily and business life. Accordingly, consumer rights, data protection as well as regulatory bodies in internet governance and the pharmaceutical sector need to coordinate and collaborate to allow for innovation while protecting consumer safety.

The proposed IGF Workshop addresses implementation of the Brussels Principles that seek to develop standards based on safety by design and multi-stakeholder collaboration to improve access to medicines and advance the goal of the UN Human Rights Council Resolution on the right of everyone to the enjoyment of the highest attainable standard of physical and mental health, including access to essential medicines.

This session will introduce and debate a set of guidelines and standards that aim to promote the right to health while contributing to the on-going struggle to rid the internet of rogue actors that sell falsified or substandard medicines, often without a valid prescription.

Relevance to Internet Governance: The internet has served as a disruptive force to traditional industry in the practice of pharmacy and trade in pharmaceutical products, allowing for the international sale of medicines to patients upon receipt of a valid prescription. A new, comprehensive model, which recognizes and reflects how consumers comparison shop on the internet in the 21st Century, is required to create a safe and affordable solution for millions of internet users. Failure to regulate the sale of medicines over the internet, including failure to differentiate between legitimate online pharmacies and rogue websites, poses a major moral hazards and public health risk.

Self-regulating online pharmacy practices, which include adherence to globally accepted pharmacy standards that ensure patient safety, are a mainstay of the safe online sale of medicines especially where online pharmacies have submitted to standards and rules of competent private credentialing organizations.

Ethical online ecommerce, appropriate internet governance, and trade in medical products has relied on its participants following national regulations of safe pharmacy practice to which they are subject, but which are sometimes at cross purposes with the laws governing transnational transactions, the pharmacies and patients they serve.

Format:

Round Table - U-shape - 90 Min

Description: The session will open with a segment that will identify: (a) the lack of evidence, exacerbated by evidence gaps, misinformation and inflamed rhetoric about the dangers surrounding importation of safe and affordable medicines; (b) the absence of a shared, internationally-recognized standards in the online pharmacy space; and (c) the realities of what is happening in the online pharmacy marketplace. Expert panelists on digital rights, public health, access to medicines, and internet distance care – along with those in attendance at our session – will describe the current state of how innovation, shadow regulations and internet governance impact access to medicines and public health.

The factual presentation will cover information both about dangerous websites that sell falsified and substandard medicines intentionally or due to negligence, and the policies of legitimate internet pharmacies that follow good standards of practice in accordance with local or international regulations.

The second segment of the Workshop will invite discussion on the output of the research agenda on transnational internet pharmacies from the perspective of governance and comparative policy analysis, in the form of Standards and Guidelines that underpin the Brussels Principles.

The goal of the organizers and Dr. Ahmad and Dr. Kohler's research agenda is to move beyond the Principles to drafting standards and model legislation; the purpose of the IGF Berlin 2019 Workshop, however, will be to engage stakeholders and civil society in a larger discussion about appropriate governance practices that incorporate digital inclusion (in its broadest definition) and consumer safety, appropriately meeting critical

needs of internet users today and into the future. The panelists will also detail the substantive policy decisions that have been developed, including the impact these policies will have on consumers and the online pharmacy marketplace.

The third segment of the Workshop is committed to summing up the views expressed by participants, with clear identification of suggested outcomes and next steps. The moderator will manage the discussion in a manner that encourages engagement and interactivity both with those that are participating in the room and online.

Expected Outcomes: The discussion, inputs and feedback from participants will:
1. Contribute to, and enhance a working model of Standards and Guidelines that build on the Brussels Principles for the Sale of Medicines Over the Internet;
2. Support the examination of pros and cons of how the internet can become a safe marketplace that promotes access to safe medicines;
3. identify both risks and opportunities, and suggested inputs to such entities as national regulators and the World Health Organization; and
4. Advance a set of multi-stakeholder global standards that make delivery of safe and affordable medicines dispensed over the internet a reality.

More generally, this Workshop will provide a platform for development for the potential of a dynamic coalition and ongoing dialogue to improve coordination and collaboration between academics, internet governance bodies, national pharmacy regulators, as well as international organizations such as the WHO and the OECD.

Discussion Facilitation:

Online Participation: The moderator will field queries when online participants wish to engage. The panel moderator will encourage online participation throughout the discussion, and incorporate their input appropriately.

Discussion facilitation: Led by the session moderator, the invited experts will be asked questions regarding key takeaways about how the access to medicines could be advanced with and multi-stakeholder developed standards. The discussion will investigate international agreements and the worrying lack of coordination and communication between the health, pharmaceutical and internet governance bodies.

The moderator will then turn the panelists to ask each other a round of questions, and then turn to the audience for an interactive discussion, dialogue and development of practical opportunities for coordination and collaboration.

Online Participation:

The moderator will field queries when online participants wish to engage.

The panel moderator will encourage online participation throughout the discussion, and incorporate their input appropriately.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption

Background Paper

IGF 2019 WS #95 Tackling Cyberbullying on Children with Digital Literacy

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Child Online Safety
Human Rights

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Intergovernmental Organization, Asia-Pacific Group

Speaker 1: Kamala Adhikari, Civil Society, Asia-Pacific Group
Speaker 2: Jutta Croll, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Cynthia McCaffrey, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 4: Xiaolei Tang, Private Sector, Asia-Pacific Group
Speaker 5: MENGCHEN GAO, Civil Society, Asia-Pacific Group

Policy Question(s):

1) Why cyberbullying is essential to be taken seriously by international community and what is the bottleneck to solve this problem?
2) Who/ which stakeholder is primarily responsible for protecting children from cyberbullying?
3) To what extent can digital literacy education increase the capacity of resilience and self-protection of children from cyberbullying?
4) What are the role of each stakeholder, including parents, educators, governments, law enforcement, civil society, private sector and children themselves, in improving children's digital literacy, and how can they cooperate with each other?
5) Why it is crucial to involve the perspective of children and their right in solving this problem and what unique contribution could be made by children?
6) Prevention and cure, which is more important in protecting children from cyberbullying? How to balance the preventive measures with the right of children to use internet and freedom of speech?

Relevance to Theme: The rapid proliferation of information and communications technology (ICT) is an unstoppable force changing the world order and shaping everyday life. Childhood is no exception, representing a generation that grows up online. Over 40 per cent of the young people polled began using the Internet before they were 13-years-old. The report by UNICEF also indicates the time online of connected children and way of using are becoming longer and more mobile. Social entertainment and learning, information and exploration and civic engagement and creativity are the main online practices of children. Moreover, the Internet has become a fixture of young people's lives regardless of income level. According to the International Telecommunications Union (ITU), while 94 per cent of young people aged 15-24 in developed countries are online, more than 65 per cent of young people in developing countries are online.

On the other hand, this online proliferation comes with increased risk, particularly for children, who are more impressionable, emotional and more vulnerable to online violence than adults are, for example, to suffer social and academic loss. Digital connectivity has made children more accessible through unprotected social media profiles and online game forums. The dangers posed by online violence, cyberbullying and digital harassment affect 70.6 per cent of young people aged 15 to 24 years old who are online globally. Cyberbullying can cause profound harm as it can quickly reach a wide audience, and can remain accessible online indefinitely, virtually 'following' its victims online for life, forming a continuum of damaging behavior. Victims of cyberbullying are more likely to use alcohol and drugs, to experience in-person bullying, to receive poor grades and to experience low self-esteem and health problems. In extreme situations, cyberbullying has led to suicide. However, evidence from UNESCO's study shows that 62% of interviewed digital users did

not know or were unsure about where to find help when cyberbullied. Consequently, it is urgent and necessary for international society to tackle and prevent violence against children and adolescents online.

Whereas in the offline world, children being bullied could escape such abuse or harassment by going home or being alone, no such safe haven exists for children in a digital world. Online bullying is carried and spread widely by mobile devices and social media. It also allows perpetrators to remain anonymous, thus reduces their risk of identification and prosecution, but has tangible repercussions in a single click, instantly disseminate violent, hurtful or humiliating words or images without legal consequence. Therefore, cyberbullying can hardly be prevented from the source, the offenders, or be intervened in the transmission media. The key to solve the problem is to minimize the harms and effect of bullies on young victims by improving their capability to protect, adapt and become resilient, so that to develop children's digital literacy, which indicates here having the skills to access, understand, question, critically analyze, evaluate and create media.

Furthermore, cyberbullying undermines the full achievement of the Sustainable Development Goal 4 on quality education, Goal 3 on good health and well-being and Goal 16 on peaceful and inclusive societies. Traditional bullying and online bullying are closely connected, both denying equal access to education and acting against the provision of safe, non-violent and inclusive learning environments for all children and adolescents (SDG 4 target 4.a). It could also increase the likelihood of narcotic drug abuse, harmful use of alcohol and the risk of mental health problems (SDG 3 target 3.4&5). In addition, cyberbullying is a kind of violence against children, which could undermine social order and security (SDG 16 target 2).

To sum-up, in order to build a healthy and positive digital environment beneficial to children, the workshop seeks to examine to what extent cyberbullying can be tackled and intervened through children's digital literacy, and how to improve their digital literacy.

Relevance to Internet Governance: If we decompose and analyze the occurrence process of cyberbullying, it contains three main elements, which are the source of bullies, so-called perpetrator or offender, the transmission media and the victim. Firstly, the potential for bullies hides behind a nameless profile disseminating violent, hurtful or humiliating words or images online. It also allows offenders to be anonymous, reducing their risk of identification and prosecution, expanding their networks, increasing profits and pursue many victims at once. Considering the measures to prevent cyberbullying from it source, it could lead to contradiction with other problems, like freedom of speech. Offenders might come from all kinds of age groups, regions and backgrounds. Therefore, cyberbullying can hardly be prevented or controlled from the source. Even though, raising the awareness of spiteful speech and remark, improving digital literacy, and building a well-ordered international cyberspace are always important.

Secondly, concerning the transmission media of cyberbullying, digital connectivity has made children more accessible through unprotected social media profiles and online game forums. Moreover, once bullying content is posted, deleting it is difficult, which increases the risk of victims being revictimized and makes it hard for them to recover. Although technology tools like Big Data and AI could be applied to filter and intercept some of the bullying words, the spreading ability of social media and the high cost lead the feasibility and effectiveness of these technology tools to be questionable.

The breakthrough point of this problem thus concentrates on the victim, to minimize the harms and effect of bullies on young victims by improving the capability to protect, adapt and become resilient themselves. Children who are digital literate are more aware of the way media content is made, where it comes from and what its purpose is, and more confident about voicing their opinions about media. They're also safer online and less likely to be manipulated by the media.

In order to improve children's digital literacy, it is important to promote the engagement and cooperation among all stakeholders in this issue, involving children themselves. Parents, as the guardian of the child, are responsible to talk to their children about online safety, make sure children understand online risks and what to do if they find themselves in trouble. Educator also plays a crucial role to incorporate information on digital safety into the curriculum and provide school-based counsellors and peer-to-peer support for children. Moreover, it is important for government to implement law and regulation to protect children online,

and businesses should enhance their awareness of social responsibility and development more preventive and child-friendly technology tools. Last but not least, children themselves also play an irreplaceable role of supporting one another by sharing information about how to protect each other, and speaking out against online violence. The majority of adolescents recognize online dangers exist and more than half think friends participate in risky behaviors, and more adolescents turn to friends than parents or teachers when they feel threatened online. Therefore, the role and capacity of children themselves should not be underestimated.

To conclude, protecting children online requires holistic and coordinated responses that take account of the full circumstances of the child's life and the wide range of players, including parents, teachers, governments, law enforcement, civil society, private sector and children themselves. Accordingly, the workshop is going to discuss the different function and responsibility of each stakeholder and how to promote the collaboration and cooperation of the entire society to protect children from online bullying.

Format:
Round Table - Circle - 90 Min

Description: In order to examine to what extent cyberbullying can be tackled and intervened through the improvement of children's digital literacy, and how to improve their digital literacy, the workshop will first of all analyze what are the underlying causes of cyberbullying, as well as the elements and links in the process of transmission, in order to explore the main factors involved in this problem. Then, aiming at improving children's digital literacy, what role can be played by different stakeholders including parents, school, government, businesses and children and how can they contribute to this issue will be discussed. A detailed schedule is designed as follow:
1.【5 mins】Welcome: Introduction to the workshop by the moderator, explain what is cyberbullying, the actuality of this problem and its harms to children.
2.【5 mins】Story Telling: Invite a child to share his or his peers' experience from children's perspective
3.【20 mins】First Round Question and Discussion: What are the underlying causes of cyberbullying? How could we tackle and prevent cyberbullying? Why digital literacy is essential in addressing this issue?
1) Open Q&A: The moderator will raise some questions for open answer and discussion from all participants, and then show the results of survey.
2) Speaker 1: Invite an expert in this field to explains the questions above.
3) Speaker 2: Invite a educator to talk about media literacy education at present.
4.【40 mins】Second Round Question and Discussion: What are the responsibility and role of different stakeholders including parents, school, government, businesses and children in this issue and how can each of them contribute to the improvement of children's digital literacy?
1) Open Q&A: The moderator will raise some questions for open answer and discussion from all participants, and then show the results of survey.
2) Speakers: Invite a representative from each stakeholder group to share their views on the questions above
5.【10 mins】Open discussion and Q&A: all participants will have a chance to ask questions and speak about their views and speakers will answer these questions.
6.【10 mins】 Summary and Closing: Closing remarks by the moderator

Expected Outcomes: First of all, the workshop aims to enhance the awareness of all stakeholders in the international society, especially in developing countries to cyberbullying and the importance of children's digital literacy and to take coordinate actions to protect children from cyberbullying.
Secondly, the workshop seeks to clarify the responsibility and division of each stakeholder in improving children's digital literacy, and to promote the cooperation of entire society.
Thirdly, the workshop is designed to underline the engagement of children in the issue in order to be keenly aware of their feeling, experience and opinions.
Furthermore, the workshop wish to facilitate the developing countries to design and implement laws and policies that protect children from online violence, bullying and abuse.
In addition, the workshop plans to promote education sector to incorporate information on digital safety and media literacy education into the curriculum that is suitable for the characteristics of each country.

Discussion Facilitation:

This workshop is planned to be an interactive session with meaningful discussion, and the discussion will be facilitated in the following ways.
Speakers: Speakers been invited to the workshop are from a diverse regions, age groups and academic backgrounds, covering every stakeholder in this issue as possible as we can, including parent, educator, business representative, expert, civil society and children themselves, in order to take all kinds of perspectives into consideration. The workshop give an opportunity for free discussion between different stakeholders. We fully respect the diversity, to be more specific, here there are 3 women and 2 men; 3 from Asia-Pacific group, 1 from WEOG and 1 from intergovernmental organization; 2 from civil society, 1 from technical community, 1 from private sector and 1 from intergovernment organization; and 1 from child group under 18--which ensure the discuss value and interaction.
Moderator: The moderator is well informed and experienced in animating multi-stakeholder discussions, and able to have a good control over the meeting progress. Questions and input for speakers will be prepared in advance to help stimulate interactive, dynamic dialogue. The moderator of the workshop will at the beginning take a roll call of all the participants and their affiliations, so that the moderator can call on individuals to comment on subject pertaining to their interest. Moderate will prep all speakers ahead of time and ask meaningful questions. He will encourage active engagement throughout.
Organizers: CFIS is a NGO and UNICEF is an inter-governmental organization.
Site design: The workshop room will be arranged as a concentric circles pattern. The invited speakers will sit in the inner circle and each of them will have a name tag in front, on which the stakeholder the speaker belongs to will be highlighted. Other participants are welcome to site from the inside to out with name tags and microphones as well.
Tools:
1) Preliminary survey: Before the workshop, targeting on cyberbullying and children's media literacy, we will do a survey with a series of questions which are designed for discussion during the workshop in order to provide first-hand and data support to workshop discussion.
2) Warm-up discussion forum: On June 1st, we will held a forum on Protection of Children Online with the UNICEF and research institute together. During the forum, sub-topics including cyberbullying will be discuss by relevant experts, which will provide professional knowledge and support to the workshop.
3) Story-Telling Session: This special session is design to give an opportunity to children to have a voice in this issue and to take their perspective into fully consideration.
4) Question and Open discussion: During the workshop, two rounds of question and open discussion are design to encourage every participant to share their views and make contribution to the issue.
5) Audio-visual material: Organizers will explore the use of visuals (i.e. videos, PowerPoint slides, images, infographics) not only for presentation, but also throughout the workshop to animate the session and aid those whose native language may not be English.

Online Participation:
The workshop encourages online participation to animate discussions in the room and online simultaneously. This arrangement is especially aimed at covering all kinds of stakeholders in our discussion, because some of them might not able to come for some objective reasons. Remote participants will also be given an opportunity to ask and answer questions during discussion.
The remote moderator will have a key role as facilitator to the online participants. He will be involved throughout the workshop planning to advise on where remote participation will need to be facilitated. The moderator will frequently communicate with the remote moderator throughout the session to ensure remote participants' views/questions are reflected. We will ensure that the workshop is advertised in advance to the wider community so that remote participants have the opportunity to prepare questions and interventions in advance and possibly generate more interested parties.

Online Participation:

The workshop encourages online participation to animate discussions in the room and online simultaneously. This arrangement is especially aimed at covering all kinds of stakeholders in our discussion, because some of them might not able to come for some objective reasons. Remote participants will also be given an opportunity to ask and answer questions during discussion.

The remote moderator will have a key role as facilitator to the online participants. He will be involved throughout the workshop planning to advise on where remote participation will need to be facilitated. The moderator will frequently communicate with the remote moderator throughout the session to ensure remote participants' views/questions are reflected. We will ensure that the workshop is advertised in advance to the wider community so that remote participants have the opportunity to prepare questions and interventions in advance and possibly generate more interested parties.

Proposed Additional Tools: Tools:
1) Preliminary survey: Before the workshop, targeting on cyberbullying and children's media literacy, we will do a survey with a series of questions which are designed for discussion during the workshop in order to provide first-hand and data support to workshop discussion.
2) Warm-up discussion forum: On June 1st, we will held a forum on Protection of Children Online with the UNICEF and research institute together. During the forum, sub-topics including cyberbullying will be discuss by relevant experts, which will provide professional knowledge and support to the workshop.
3) Story-Telling Session: This special session is design to give an opportunity to children to have a voice in this issue and to take their perspective into fully consideration.
4) Question and Open discussion: During the workshop, two rounds of question and open discussion are design to encourage every participant to share their views and make contribution to the issue.
5) Audio-visual material: Organizers will explore the use of visuals (i.e. videos, PowerPoint slides, images, infographics) not only for presentation, but also throughout the workshop to animate the session and aid those whose native language may not be English.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #99 Towards a Multistakeholder Cybersecurity Framework

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
International Norms
Domain Name System

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Johannes von Karczewski, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Ludmilla Georgiew, Private Sector, Western European and Others Group (WEOG)
Speaker 3: Jan Neutze, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Marina Kaljurand, Civil Society, Eastern European Group
Speaker 5: Anriette Esterhuysen, Civil Society, African Group

Policy Question(s):

1. Norms for good behaviour of state and non-state actors in cyberspace
2. Collaboration among various private sector and governmental initiaves (Paris Call, Tech Accord, Charter of

Trust, GCSC, GGE/OEWG, Contract for the Web etc.) to enhance cybersecurity,
3. Development of a Multistakeholder Global Framework for Cybersecurity and Digital Cooperation

Relevance to Theme: Discussions on norms for the behaviour of state and non-stae actors in Cyerspace have been intensified since the failure of the UNGGE in 2017. Numerous activities by the private sector as well as by governments has been launched in recent years aimed at more cyberstabilty and enhanced cybersecurity as the Paris Call, the Global Commmission on Stability in Cyberspace, Microsofts Tech Accord and Digital Peace Campaign, Siemens Charter of Trust etc.

Relevance to Internet Governance: Security, stability and resilience on cyberspace is since the start of the IGF in 2006 a key issues of Internet Governance

Format:
Break-out Group Discussions - Round Tables - 90 Min

Description: Towards a Multistakeholder Cybersecurity Framework: How to translate multiple plans – from the Charter of Trust to the Paris Call - into one global pratice.

Recent Cyberattacks againts core elements of the Internet infrastructure have the dangerous potential to undermine stability in cyberspace. Freedom of communication, digital trade and many other activities of today´s life are dependent from a functioning Internet. This is recognized both by states and non-state actors around the globe, however so far there is no global agreement among stakeholders how to keep the vybersdpace stable and secure.

In the last two years a number of initiatives to stabilize cyberspace and to avoid a new generation of cyberconflicts has been launched both by various governments and the private sector. The Paris Call for Trust and Security in Cyberspace (initiated by the French government) got meanwhile the support of more than 60 governments and around 500 non-governmental actors. The Dutch government initiated in 2017 the establishment of the Global Commission on Stability in Cyberspoace, which has proposed a so-called „Norm Package“ to enhance cybersecurity. The Charter of Trust (initiated by Siemens) as well as the Tech Accord and the Cyber Peace Campaign (both initiated by Microsoft) got broad support from governments and non-governmental stakeholders. In June 2019 the final report of the UN High Level Panel on Digital Cooperation will also make recommendations to contribute to security, stability and resilience in cyberspace.

All this are good examples, how the multistakeholder approach to Internet Governance, as proposed by the Tunis Agenda (2005) is translated into concrete actions and how governments, the private sector, the technical community and civil society are working hand in hand to keep the Internet, free, open, unfragmented and peaceful.

The two new intergovernmental committees, established by the 73rd UN General Assembly in December 2018 (GGE & OEWG) have now a concrete mandate to negotiate arrangements to enhance cybersecurity on a global level. They are also invited to enter into broader consultations with non-state actors and regional organisations.

The proposed workshop will bring experts from the various projects together and will discuss, how the state and non-state initiatives can support each other and contribute to the emergence of a global framework for cybersecurity and digital cooperation and to stop the militarization of cyberspace and to enhance cybersecurity.

Conveners:
Charter of Trust/Siemens, Global Commission on Stability in Cyberspace, Google,

Session Organizers:
Wolfgang Kleinwächter, GCSC, Max Senges, Google, Johannes von Karczewski, Siemens

Speakers:
Johannes von Karczewski, Siemens

Ludmila Georgieva, Google
Anriette Esterhuysen, APC, South Africa
Jan Neutze, Microsoft
Marina Kaljurand, Global Commisison on Stability in Cyberspace, MP, Estonia

Additional Resource Persons:
Carmen Gonsalvez, Dutch Ministry for Foreign Affairs (TBC)
Christoph Meinel, Hasso Plattner Institute Potsdam
Isabel Skierka, Digital Society Institute, Berlin (TBC)
Chris Painter, former Cyber Coordinator of the US Department of State

Moderator:
Wolfgang Kleinwächter, GCSC (Offline) / Alexander Klimburg, The Hague Center for Strategic Studies (Online)

Rapporteur:
Louk Fassen, GCSC

Expected Outcomes: 1. Enhanced collaboration among the various state and non-state cybersecurity initiatives
2. Development of a Proposal for a Multistakeholder Global Framework for Cybersecurity and Digital Cooperation (New Deal)

Discussion Facilitation:

The format will be a round table discussion with a moderator who will encourage interventions from the floor as well as online. A background paper will be distributed online before the workshop

Online Participation:

A background paper will be distributed online before the workshop

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #118 Public Interest Challenges in governing Geo Top-Level Domain

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Domain Name System
Internet Resources
Trust and Accountability

Organizer 1: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Wolfgang Kleinwaechter, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Lousewies van der Laan, Technical Community, Western European and Others Group (WEOG)

Speaker 3: Jorge Cancio, Government, Western European and Others Group (WEOG)
Speaker 4: Marianne Georgelin, Government, Western European and Others Group (WEOG)
Speaker 5: Dirk Krischenowski, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

What are the Key Public Interest Challenges in governing geographic Top-Level Domains (geoTLDs)?
What do we currently see as best practice in governing geoTLDs?
Which model is more feasible for governing geoTLDs: a private or a governmental model?
How can geographic names be protected for a reasonable use as public identifier?

Relevance to Theme: Over 60 new geographic top-level domains (geoTLDs) from allover the globe have become digital identities for cities, regions and cultural and language communities so far. The local geoTLDs like .corsica, .tokyo and .quebec complement the national country code extensions like .fr, .ca and .jp.

Relevance to Internet Governance: With the operation of geoTLDs city and regional governments have become new stakeholders in the governance of critical Internet infrastructures and services. The public and private governance models of the geoTLDs differ with the level of interaction with the place's stakeholders which are mainly the relevant government and private companies, but also citizens, culture, academia, science and the technical community.

geoTLDs also touch a broad range of public interest aspects, including the protection of geographic names on the Internet. More geoTLDs will be introduced once ICANN opens a new application round.

Format:
Debate - Classroom - 90 Min

Description: The issue of the proposed debate is to identify key public interest challenges (such as trust, accountability, security, geonames) and exchange best practice in governing the place's digital home. The debate format is designed for a balanced interaction of participants from relevant stakeholders from a broad variety of countries including the audience.

The debate setting is:
1-2 participants from local governments operating a geoTLD
1-2 participants form private sector organisations operating a geoTLD
2 judges from academia, internet user community, others
1 moderator

Expected Outcomes: The debate is designed to contribute to a better understanding of the challenges in governing public geographic identifiers such as city and regional names on the Internet. This includes policy and governing aspects, intellectual property rights and economic challenges.

The debate also aims to educate what the key factors that make a geoTLD a success for the place, its inhabitants and the government.

Discussion Facilitation:

We are going to invite a large community of stakeholder in the topic through our channels with ICANN, ISOC, city governments and others.

Online Participation:

We would like to use the official Online Participation Platform which means live streaming.

Proposed Additional Tools: May be we use Skype/Threema/Periscope as further access and participation tools.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities

Background Paper

Reference Document

IGF 2019 WS #131 Quantifying Peace and Conflict in Cyberspace

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Internet Resources
Trust and Accountability

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, African Group
Organizer 4: Private Sector, Western European and Others Group (WEOG)
Organizer 5: Private Sector, Eastern European Group

Speaker 1: Izabela Albrycht, Government, Eastern European Group
Speaker 2: Praveen Abhayaratne, Civil Society, Asia-Pacific Group
Speaker 3: Marilia Maciel, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 4: Liga Rozentale, Private Sector, Eastern European Group
Speaker 5: Trust Mamombe, Civil Society, African Group

Policy Question(s):

How can data on cyber peace help inform policymaking?

What publicly available data sources exist to measure the levels of peace in cyberspace?

What are the indicators and elements needed for contributing to peace in cyberspace?

What role can civil society, SMEs and the tech industry have in creating more peace in cyberspace?

Relevance to Theme: Safety and security in cyberspace are prerequisites to economic growth and a healthy digital ecosystem for all users, governments, businesses, civil society and academics alike. Under this theme, strategies for mitigating the risks and strengthening security will be addressed through the lens of data-backed approaches to quantifying the impacts to conflict in cyberspace. An accurate diagnosis is the basis for an effective policy response – and yet, to date, limited progress has been made on accurately measuring the impact of cyber conflict and corresponding potential for cyber peace on society.

Relevance to Internet Governance: This session will help create more accuracy in diagnosing the state of conflict in cyberspace by gathering data on the indicators that feed into peace in cyberspace. This diagnosis will ultimately help feed into the development of rules, norms and principles to help shape the future of cyberspace.

Format:

Other - 60 Min
Format description: This session will merge the “tutorial” and “roundtable” formats in order to adapt to a

topic of a policy pitch. The session will begin with the tutorial in which the Institute for Economics and Peace will do a deep dive on how their organization creates the Global Peace Index, their findings for 2018, and how the findings help inform policymakers around the world. Next, the session will move into a moderated roundtable discussion once participants have the baseline understanding of data and economic analysis for peace.

Description: Instability in cyberspace is rising with the increasing number of countries and non-state actors weaponizing technology. Today, the threats posed by cyber-attacks have the potential to disrupt everything from critical infrastructure, to elections, to the societal structures of our everyday lives. Despite the fact that cybersecurity touches news headlines and diplomatic agendas around the world, there has been limited progress on understanding the impact of conflict in cyberspace on the functioning of society. Moreover, even less is understood regarding the relationship and interdependencies between business, peace, prosperity, culture, economy and politics in cybersecurity.

Efforts to measure peace, such as the index compiled annually by the Institute for Economics and Peace (IEP), allows us to assess the social, political, and economic factors that create peace. Over the past several years, progress has been made in measuring the various indicators associated with violence, conventional weapons proliferation, crime and armed conflict, which has helped governments make more informed decisions regarding public policies.

An accurate diagnosis is the basis for an effective policy response – and yet, to date, limited progress has been made on accurately measuring the impact of cyber conflict on society. For example, Northern and Western Europe often appear at the top of the lists in rankings of peaceful countries, how would those rankings differ if measured only on their levels of cyber peace?

Panelists will discuss efforts such as the Diplo Foundation's Data Diplomacy project and the IEP's framework of measuring Positive Peace, which describes the attitudes, structures and institutions that underpin and sustain peaceful societies. Drawing from the various data-backed approaches to public policy, this panel will discuss what is needed to create and measure Positive Peace in cyberspace. The conversation is intended to bring together experts on peace and cybersecurity to exchange views and reflect on the opportunities for quantifying peace in cyberspace in order to better inform policy decisions.

Proposed agenda

- Tutorial: Using open source data to quantify global peace (10 minutes)

o How to measure peace

o Findings from the 2018 Global Peace Index

- Roundtable discussion: How to measure peace in cyberspace (30 minutes)

o Trends in cyber conflict today

o Data indicators for cyber conflict, from cyber crime to development of cyber weapons to the prevalence of legislative and institutional frameworks on cyberecurity

o What role can civil society, SMEs and the tech industry have in creating more peace in cyberspace?
- Open Mic Session (10 minutes)
- Conclusion: What is the path forward towards creating an index for measuring peace and conflict in cyberspace? (10 minutes)

Expected Outcomes: This workshop is designed to provide input into the existing data sources and identify remaining gaps that contribute to the lack of understanding around the quantifiable impact of threats in cyberspace. The panelists will discuss the benefit of a global cyber peace index and how its findings may or may not differ from mappings of global peace against traditional forms of conflict.

Discussion Facilitation:

An open mic session follows the main session to enable the audience and remote participants to join the conversation and present their experiences, opinions, suggestions, etc., on how to move the debate forward. Audience discussants will either queue at their stakeholder-assigned mics, or the panel rapporteurs will bring the mics to discussants, and rotate, with online participants having their own equal queue.

Online Participation:

We will have two online moderators to assist with the online conversation. To broaden participation, social media (Twitter and Facebook) will also be employed by the on-line moderators who will be in charge of browsing social media using a designated hashtag.

Proposed Additional Tools: We would also like to offer an additional accessible platform in order to get more involvement from remote participants, especially those who might have a disability. Microsoft Teams, for example could be offered as a place for additional discussion before and after the panel through setting up a dedicated Teams channel for the panel. Using Microsoft Teams during the panel would enable us to turn on accessible features such as screen readers, translator and captions.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #135 Attacks against to Public Core. Can the Internet survive?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
International Norms
Domain Name System

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Technical Community, Western European and Others Group (WEOG)
Organizer 4: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Olaf Kolkman, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Andrei Kolesnikov, Technical Community, Eastern European Group
Speaker 3: Marina Kaljurand, Civil Society, Eastern European Group
Speaker 4: Anriette Esterhuysen, Civil Society, African Group
Speaker 5: Ram Mohan, Technical Community, Asia-Pacific Group

Policy Question(s):

1. What are the new threats for the basic technical functioning of the core of the Internet (Servers, DNS, IP Adresses, Protocols, Codes, Cables, Satellites)?
2. How the international Community should react to a new generation of attacks against the public core of

the Internet?
3. What are the special responsibilities of governments, private sector, technical community and civil society (cyberhygiene)?

Relevance to Theme: The theme is of growing relevance against the background of new forms of attacks against the root and name server system (DNSHijacking/DNSpionage/Netnow/IRA). There are also new threats for the functioning of the core of the Internet by unintended side effects of national legislation (data localisation, cybersovereignty, national segments etc.) and new technological innovations (DOH, DOA, Blockchain)

Relevance to Internet Governance: The management of critical Intenet resources as root and name server, the DNS and IP Adress System etc. are a key aspect of Internet Governance.

Format:
Round Table - U-shape - 90 Min

Description: Proposal

Attacks against the Public Core: Can the Internet survive?

The stability of the Internet is based on the functioning of the key elements of the Internet architecture – the root- and name-server system, the Domain Name System (DNS), the IP-Address system, Internet protocols, codes, cables and satellites. Those technical elements constitute the public core of the Internet and enable the communication among the millions of connected networks and billions of connected computers with all the applications and services which run over the DNS.

The root server system, DNS, IP addresses, Internet protocols and other elements of the technical core of the Internet are managed in a neutral way by the global Internet community itself, coordinated by ICANN, RIRs, RSSAC, IETF, W3C and other non-governmental entities.

Criminal attacks against the DNS are not new, however, in recent years, attacks became more sophisticated and aggressive, as the DNS Hijacking case (DNSpionage) against Netnod in January 2019 has demonstrated.

Another new threat for the public core of the Internet emerges from a more politically motivated process. More and more governments introduce security measures to protect their so-called “national Internet segment“ to strengthen their „cybersovereignty“. Such legislation can have unintended side effects which have the potential to undermine the neutral functionality of the global server system when local operators are pushed into a situation that their global commitments – as the principles of neutrality and impartiality for root server operators – conflict with national legislation.

There can be also unintended side effects for the functioning of the public core of the Internet by the development of new innovative technologies as DOH, DOA, Blockchain and others.

Furthermore, we have seen a new type of offensive cyberattacks in intergovernmental conflicts. The New York Times reported in January 2019 about an attack against servers of the Russian troll factory, the Internet Research Agency, in St. Petersburg to block a potential interference into the US Congressional elections in November 2018.

Such new threats for the global functioning of the technical core of the Internet have the potential to undermine the stability in cyberspace with far reaching political and economic consequences. To reduce such a threat the Global Commission on Stability in Cyberspace (GCSC) has proposed the adoption of an international norm to protect the public core of the Internet. The proposed norm reads as follows: “Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.”

The language of this proposed norm, although still under discussion, has been meanwhile included in various political documents as into resolutions of the European Parliament, into the EU Cybersecurity Directive and into the Paris Call for Trust and Security in Cyberspace, initiated by the French government in November 2018.

During the recent ICANN64 meeting in Kobe (March 2019), the GCSC had a series of consultations with ICANN constituencies, including the Security and Stability Advisory Committee (SSAC) and the Root Server System Advisory Committee (RSSAC) about the implementation of the norm by proposing an enhanced cyberhygiene in the DNS, and in particular by server operators and service providers.

The proposed IGF workshop will look deeper into the issue by specifying the threats and potential sagefuards against this new generation of attacks. The workshop will also discuss how the implementation of „good practice“ and an enhanced cyberhygiene can contribute to the protection of the public core of the Internet to stabilize cyberspace and what roles and responsibilities emerge from those new threats for governments, the private sector, civil society and the technical community.

Conveners:
DENIC, Afilias, Global Commission on Stability in Cyberspace,

Session Organizers:
Wolfgang Kleinwächter, GCSC, Jörg Schweiger, DENIC, Philipp Grabensee, Afilias

Speakers:
Olof Kolkman, ISOC
Ram Mohan, Afilias
Marina Kaljurand, Global Commisison on Stability in Cyberspace, MP, Estonia
Anriette Esterhuysen, APC, South Africa
Andrej Kolesnikow, SSAC/ICANN

Additional Resource Persons:
Abdul-Hakeem Ajijola, CSS, Nigeria
Marjette Schaake, Member of the European Parliament, The Netherlands
Virgillio Almeida, former ICT Minister, Brazil
Chris Painter, former Cybersecurity Coordinator, US Department of State
Frederick Douzet, Sorbonne University Paris, France

Moderator:
Wolfgang Kleinwächter, GCSC (Offline) / Alexander Klimburg, The Hague Center for Straegic Studies (Online)

Rapporteur:
Peter Koch, DENIC, ISOC Germany

Expected Outcomes: Further specification of the Norm to Protect the Public Core of the Internet, as proposed by the GCSC, and to develop it into a proposal for the forthcoming UN negotiations under the GGE/OEWG.

Discussion Facilitation:

There will be very brief statement by the speakers to allow an interactive discussion among the speakers and and early engagement of the broader public, offline and online.

Online Participation:

We will publish a background paper in mid-November to enable participants to prepare for the workshop

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #137 Kids online: what we know and can do to keep them safe.

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
Hate Speech
Human Rights

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 3: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 4: Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)

Speaker 1: AMANDA THIRD, Technical Community, Asia-Pacific Group
Speaker 2: Alexandre Barbosa, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 3: María Alejandra Erramuspe, Government, Latin American and Caribbean Group (GRULAC)
Speaker 4: Wenying Su , Intergovernmental Organization, Asia-Pacific Group

Policy Question(s):

What do we know?
• According to the available evidence, what are the current trends in the activities that children perform online? What risks do they experience online?
• Specifically, to what extent are children exposed to harassment and hate speech online? What are the singularities of these issues considering gender?
• What do children have to say about their own safety online?

What needs to be done?
• How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and sexual abuse in the online environment?
• How can children´s resilience be increased by means of capacity building, media literacy, support and guidance in the digital environment?
• What legal, regulatory and technical instruments need to be put in place to meet the needs of the children and harness digital opportunities for them?
• How can children's rights be embedded in the activities and policies of international Internet governance institutions? How can the gender perspective be integrated within the children´s rights perspective for such matters?

How can it be done?
• What role should different stakeholders play in cybersecurity capacity building approaches?
• What multi-stakeholder collaboration arrangements have been put in place in the regions represented in the panel, and with what outcomes?
• Can these initiatives be replicated in other regions? What would be the viability and main challenges of doing so?

Relevance to Theme: In a context of increasing access to the Internet by children, where one every three Internet users is a child (UNICEF, 2017), the relevance of knowing how they use it and how they handle the risks and opportunities associated with that use is indisputable. The available data suggests a significant

diffusion of both home and mobile Internet access by children, particularly since 2012 (Global Kids Online, 2016; UNICEF, 2017). In other words, over the latest years, more children have gone online worldwide, with a shift from a predominantly middle-class access to access by poorer children (yet with great variation between countries). This means that both the risks and opportunities associated with digital inclusion have diversified, as have the knowledge, skills and behaviour patterns of the new users.

In this context, the phenomenon of massive child online presence is relatively new and, therefore, the reliable knowledge about it still scarce, particularly in the Global South. In order to formulate comprehensive policies and to implement effective protection and promotion measures targeting online children, it is germane to approach the topic from an evidence-based perspective and to avoid both unnecessarily magnifying risks and underestimating potential benefits of the digital inclusion. In this context, the reference to evidence does not merely involve considering the traditional available data sources, usually statistical data. As it has been frequently pointed out (among others, by Faro Digital NGO and UNICEF), the approaches to child online safety have almost exclusively portrayed an adult perspective. Failing to consider children´s own stake on the issue entails not only limiting their right to expressing their voice on matters that directly involve them, but it may also lead to policy and communication design flaws. In other words, projects and communication materials often speak a language and pose issues that differ from children´s understanding of them, leading to failures in reaching the target audience and, moreover, in meeting children´s needs.

An evidence-based approach to this topic needs to encompass the complexity of the issue, considering both the supply and demand sides. The former, including Internet and platform features, laws, regulations and policy measures; the latter comprising children´s perspectives, actions, skills and resources, along with those of their parent´s.

A specific value of the proposed workshop, therefore, is that discussions will be grounded on recent, nationally representative and reliable data on children´s use of the Internet and on children´s own perspective, which will be brought to the table as a result of a series of workshops organized globally to hear their voice. Furthermore, the very production of the data and the experiences showcased are framed in multi-stakeholder collaboration arrangements, representing an example of good practice in terms of what needs to be done in order to promote child safer use of the Internet and how to further harness the opportunities associated with it.

Guaranteeing opportunities for digital inclusion and lifelong learning, as expressed by SDG 4, cannot be achieved without gender equity and without meeting the gender-specific challenges faced by child internet users; therefore the direct relation of the proposed panel with SDGs 4 and 5. Moreover, keeping children safe and healthy, as expressed in SDG 3, is among the most important goals for children in the SDGs, and it entails considering the threats and opportunities posed by the online environment. Finally, ending violence against children by 2030 includes ending sexual abuse, harassment and hate speech both offline and online, something that is, in turn, key to achieving peaceful and inclusive societies, as expressed by SDG 16.

Relevance to Internet Governance: With one every three Internet users being a child, a generic or age-blind approach to “users” in Internet governance regimes, policies or regulations may certainly fall short of effectively meeting children´s needs and guaranteeing their rights, since children constitute a population with very specific developmental characteristics, vulnerabilities and rights. In this sense, this proposal is relevant since it brings children´s rights to a focus within the Internet Governance agenda. Given the 30th anniversary of the UN Convention on the Rights of the Child, in November 2019, this proposal is particularly timely to guarantee covering the topic.

Complementarily, the relevance of the proposed approach lies in the fact that by bringing together researchers, policy-makers and children´s voice to the table, it guarantees an approach characterized by a multi-stakeholder perspective, with the added value of organizing the discussion on an evidence-based approach, including children’s own voice. Furthermore, both the data production and the policy measures to be discussed have taken place, from the onset, within multi-stakeholder approaches, where collaboration between government, civil society and the academia have crystallized both in joint financing and planning of the research, and the ulterior policy discussions.

By disseminating knowledge about children´s access, use, skills, opportunities and risks faced online and stimulating the discussion about challenges and actions needed for a safer digital inclusion, the proposed workshop is also relevant to Internet Governance by pointing in the direction of feasible courses of action. Discussing rules, decision-making and programmes needed to shape the evolution of the Internet towards a safer place for children and an ambient that provides better quality opportunities to them impacts the right to digital inclusion and to quality education as expressed in SDG 4 of the 2030 Sustainable Development Agenda.

Format:

Panel - Auditorium - 90 Min

Description: AGENDA

Introduction by the panel moderator (5')
Presentations from panellists (45', of which 5' for short introductions)
• Cristina Ponte (Universidade de Lisboa, Portugal)
• Wenying Su. (Child Protection Section, UNICEF, China).
• Amanda Third (Western Sydney University, Australia)
• Alexandre Barbosa (Cetic.br, Brazil)
• Alejandra Erramuspe. (AGESIC, Uruguay).

Moderation: Guilherme Canela (UNESCO).

Comments and questions from the audience, both present and remote (45', of which 5' for final remarks)

METHODOLOGY AND FACILITATION STRATEGY

Each panellist will be previously briefed to prepare a short presentation organized on the basis of the policy questions, and bringing a regional perspective.

After the presentations, the moderator will organize a participatory discussion, raising questions linked to the policy questions and making room for questions from the audience (both present and remote), including questions from the other panellists.

Children's own voice will be present through children´s participation in the qualitative research workshops previously carried out in the frame of the facilitating children's consultations for the UNCRC General Comment on Children and the Digital Environment, in which the presenter´s organization participates.

Members of the networks dedicated to research on online children and to advocating for online children´s protection and promotion, like Global Kids Online and Latin America Kids Online will participate remotely in the panel discussions.

Expected Outcomes: - Increased visibility and awareness of children´s rights within the Internet Governance agenda.
- A thoroughly discussed and updated roadmap of the main challenges and opportunities for online children, stemming from multi-stakehorlder discussions and enriched by the audicience´s input (including both present and online participants).
-Clear identification of action paths and feasible multi-stakeholder arrangements in the regions represented.

Discussion Facilitation:

Interaction will be encouraged in the different lines:

a) Between panelists. Panelists will be encouraged to ask each other at least one question, in addition to answering the moderator´s and audience´s questions.
b) Between panelists and the audience. The audience will be able to ask questions right after each panelist intervention. Questions will be made in real time. Members of the audience who prefer to do so, will be able

to
send the moderator written questions as well.
c) From remote participants. Questions and comments from the online participation official platform and other social media (Twitter) will be compiled by a designated team member, and read right after every round of questions from the onsite audience.

Online Participation:

A moderator will be organizing the remote participation in the online tool and will be answering questions, commenting with the participants, and he will bring some of the comments or questions to the panelists and present audience.

Proposed Additional Tools: Remote participation will also be facilitated through a hashtag in Twitter.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Background Paper

Reference Document

IGF 2019 WS #141 Best practices for child protection and sexual speech online

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
CSAM
FoE online

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Malcolm Jeremy, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Catherine Gellis, Private Sector, Western European and Others Group (WEOG)
Speaker 3: Jillian York, Civil Society, Western European and Others Group (WEOG)
Speaker 4: Fauzia Idrees Abro, Technical Community, Asia-Pacific Group
Speaker 5: Takashi Yamaguchi, Private Sector, Asia-Pacific Group

Policy Question(s):

How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and sexual abuse in the online environment? How can Internet platforms of all sizes take a nuanced and better-informed approach towards content moderation and censorship, that does not over-censor legitimate sexual content such as art, fiction, sexual education material, and testimonials from survivors? How can these platforms fulfill their obligations under the United Nations Guiding Principles on Business and Human Rights to conduct due diligence that

identifies, addresses and accounts for actual and potential human rights impacts of their activities, when it comes to measures they take for the protection of children?

Relevance to Theme: The session contributes to the theme insofar as it addresses the management of risks to child safety online, while also taking a broader perspective to ensure that potential solutions do not infringe the human rights of other stakeholders, especially those who are stigmatized and marginalized, such as sex workers, adult entertainers, creators and fans of independent media, sex educators, the LGBTQ+ community, and others who have legitimate reasons for communicating sexual content online. It also concerns the need for trust and accountability of Internet platforms, who make decisions about the moderation of sexual content based on their internal policies and terms of service. In doing so they frequently make use of resources such as hash lists and URL lists that are not made publicly available, raising questions about the accountability of actions taken using these tools.

Relevance to Internet Governance: Child Sexual Exploitation Material (CSEM) is almost exclusively distributed online, and a significant proportion of the sexual grooming of minors is also conducted online. Child protection laws such as FOSTA are directed specifically against Internet platforms, and in 2019 the UK government announced the introduction of a tough new regulatory regime requiring Internet platforms to assume a duty of care to keep children safe from online harms. Also in 2019 the United Nations Committee on the Rights of the Child released Draft Guidelines on the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, which contain a number of recommendations about the responsibilities of Internet platforms. As such, this session is deeply relevant to Internet governance.

Format:

Round Table - U-shape - 90 Min

Description: Internet content platforms (such as search engines, social networks, chat applications, and cloud storage services) are frequently the first port of call for regulators seeking to find easy solutions to the problem of online child sexual abuse. But although platforms have made a vital contribution towards this effort and will continue to do so, there are at least three limitations of the approach that regulators are pushing platforms to take.

First, it tends to promote a “one size fits all” approach that overlooks the differences between platforms in terms of their financial resources and technical expertise. As the the Internet Watch Foundation (IWF) has testified to the UK government, "There is a myth that the tech industry is a-wash with money and the brightest and the best brains, with the ability to solve all the world’s problems and whilst that may be true of some of the larger players, there is a need to recognise that much of the tech industry in the UK is made up of small start-ups that do not have access to the sorts of resources Government think they do."

Second, when platforms are pushed into over-blocking and over-censoring, this frequently results in infringements of the civil liberties of minorities such as sex workers, the LGBT community, survivors of child sexual abuse, and sex workers. For example, the U.S. law FOSTA (Allow States and Victims to Fight Online Sex Trafficking Act) which was putatively aimed at making Internet platforms liable for the facilitation of sex trafficking, has in practice also resulted in the censorship of lawful speech, including sex education resources.

Third, an approach that pushes platforms into censoring any sexual content that they instinctively regard as “questionable” does not actually protect children, and could indeed harm them. Sometimes platforms choosing not to censor content is more likely to protect children from sexual abuse. For example, in response to FOSTA, threats of regulation, and public pressure, platforms have been found censoring child sexual abuse prevention materials and forums.

More broadly, United Nations Special Rapporteur David Kaye found in his 2018 report on the promotion and protection of the right to freedom of opinion and expression that the failure of platforms to apply human rights standards in their policies related to sexual content has resulted in the removal of resources for members of sexual minorities, and depictions of nudity with historical, cultural or educational value.

Currently, many platforms do already have child protection policies as part of their content policies or community standards, however these can be vague and unpredictable in their application even by a single platform, let alone between platforms. Smaller platforms may not have well-developed policies on this topic at all. Even in mid-size platforms, trust and safety teams are typically composed of members who deal with other forms of abusive content such as spam and fraud, but which lack dedicated expertise in child protection. Often, requests to block or restrict content are received from third parties, but are not adequately reviewed internally before being actioned.

Platforms of all sizes need to be empowered to be made more effective contributors towards child sexual abuse prevention, through a more nuanced and better-informed approach towards content moderation and censorship.

Unfortunately, to date two obstacles have prevented this from becoming a reality. First, many of the largest mainstream child protection organizations that have promoted platform liability rules as a solution to child sexual abuse have a broader agenda to eliminate adult content online, and they exclude perspectives of those who don't share that agenda, such as sex-positive therapists and researchers, LGBT people, sex workers, and the consensual kink community. As a result, there has been nobody to speak up when these communities become casualties of censorship such as over-blocking.

The second factor that has prevented platforms from taking a more nuanced and better informed approach towards content moderation and censorship as it relates to child protection is the powerful sexual stigma that affects all who work in this area. Although approaches based on the prevention of child sexual abuse are effective, stigma makes it difficult for this approach to make headway against the emotionally more resonant approach of identifying and prosecuting offenders. It also makes it difficult to suggest balances and safeguards for child protection laws and policies that are necessary in a free and democratic society.

Prostasia Foundation will be convening a multi- stakeholder seminar and roundtable discussion on the roles that Internet companies can take towards the prevention of online child sexual abuse, in a way that is consistent with human rights and Internet freedom. The first phase of this convening is a full-day expert-led seminar and discussion with Internet platforms, along with representatives from marginalized stakeholder groups, to be held in San Francisco in May 2019. Following this, a self-selected working group will form to work online to synthesize the learnings of the event in a draft, non-normative best practices document.

This best practices document will become the input for a roundtable workshop that is to be held at RightsCon 2019, at which we will hold a multi-stakeholder facilitated deliberation to further distill the draft best practices document into a series of normative recommendations. Finally, the best practices paper and the policy recommendations will be presented at the 2019 Internet Governance Forum with the aim of socializing them within a broader community of stakeholders, and assessing the degree of consensus that they have achieved. In addition, we will be presenting a new report on the transparency and accountability practices of major platforms, consultants and agencies involved in online child protection.

Expected Outcomes: The objective of this project is to enable industry participants to ensure that their child protection policies and practices are scientifically sound, and that they fulfil their obligations under the United Nations Guiding Principles on Business and Human Rights, which require companies to "Conduct due diligence that identifies, addresses and accounts for actual and potential human rights impacts of their activities, including through regular risk and impact assessments, meaningful consultation with potentially affected groups and other stakeholders, and appropriate follow-up action that mitigates or prevents these impacts."

By facilitating a dialogue with experts and stakeholders who are normally excluded from the development of child protection policies by Internet platforms, we aim to make these policies more evidence-informed, and more compliant with human rights standards. In concrete terms, this will be evidenced by improved accuracy in the moderation of sexual content. Specifically, participating platforms will remove more material that is harmful to children and has no protected expressive value, and less material such as lawful, accurate information on child sexual abuse prevention. The ultimate result of this will be that more children are saved from child sexual abuse.

In addition, four tangible outputs will be produced from this workshop and its preparatory events:

1. Best practices paper: The best practices document prepared in between the first and second face-to-face convenings will record the messages shared by experts, stakeholder representatives, and Internet platforms at the first convening in San Francisco. This document will include references to source materials and will guide participants at the second convening towards the development of key policy recommendations.

2. Policy recommendations: A set of policy recommendations will be finalized at the expert-facilitated follow-up event at RightsCon. Although the intention of this document is not to standardize terms of service related to child protection across the industry, it may include a set of model terms of service for Internet platforms with respect to child protection that smaller Internet platforms can easily adapt and use.

3. Transparency and accountability report: This inaugural report on the practices of Internet platforms, software vendors, and content rating agencies will become an ongoing resource for those who are affected by the child protection practices of these bodies, and provide an aspirational standard for improvements in their accountability and transparency.

4. Advisory network: The process will also result in formation of a standing advisory network of stakeholders, with secretariat support from Prostasia Foundation, who can provide advice and feedback to Internet platforms on their child protection policies and their human rights impacts.

Discussion Facilitation:

The session will be divided into three parts of approximately equal duration. During the first part, the content of the best practices paper, the policy recommendations, and the transparency and accountability report, will be outlined and questions from the onsite and remote participants will be taken. During the second part, our diverse expert panel will react and provide their perspectives and further insights, and will invite an interactive discussion from the local and remote participants. The final 30 minutes of the session will then be devoted to intensive facilitated group deliberation on the policy recommendations, to assess whether the degree of consensus that they have achieved among the session participants. During this final part of the session, the best practice recommendations developed during the preparatory meetings will be discussed point by point in a roundtable format, facilitated by the onsite and online moderators, and with note-taking by the rapporteur.

Online Participation:

Using the official online participation tool, our remote moderator will take questions and comments from remote participants. The remote moderator will be called upon in each round of questions taken from the floor, so that to the nearest extent possible, remote participants receive parity in treatment with those who are present in person. We will also use the official online participation tool to provide links to presentation files that are being displayed in the session room, so that remote participants can load these on their own computers, rather than having to view them via the webcast video.

SDGs:

GOAL 5: Gender Equality
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #144 Platforms and moderation - norms or regulation?

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

Fake News
FoE online
Human Rights

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Technical Community, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)
Organizer 4: ,

Speaker 1: Jordan Carter, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Farzaneh Badii, Civil Society, Asia-Pacific Group
Speaker 3: Maureen Hilyard, Civil Society, Asia-Pacific Group
Speaker 4: Konstantinos Komaitis, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

1. Will forcing platform operators to take legal responsibility for illegal or harmful content uploaded by their users suppress too much speech?

2. Is it reasonable to expect platforms to identify and takedown all objectionable content before it is ever aired?

3. Is the use of social media platforms by foreign governments to provide alternative views on sensitive international issues a threatening action that needs to be controlled, or a broadening of access to information?

4. Would a failure to establish norms on this subject increase the pressure for governmental regulation of platforms, the Internet, or both?

5. What is the most appropriate policy development process: Are policies solely determined by platform operators legitimate? Appropriate? Effective?

6. Should platform operators rely on their community of users for developing user policies? Should they wait for government regulations to determine how they process content?

Relevance to Theme: The security and safety of Internet users is affected by the presence of objectionable content on mainstream Internet platforms. Digital civility can be compromised. Platforms often develop their own standards or norms for how to tackle this challenge. Should citizens or governments have more of a say?

Further, global norms could help drive security and safety for all Internet users; the absence of them could inspire states to move towards a more regulatory approach with the associated risks of fragmentation

Relevance to Internet Governance: Internet platforms are a key arena of public use of the Internet and of people's participation in society. Regulatory pressures on the evolution and use of the Internet will intensify if suitable norms or regulatory approaches to platforms are not developed. As such, the outcomes of this debate will shape the evolution and use of the Internet directly.

Format:

Round Table - Circle - 90 Min

Description: In the round table, the identified speakers will share short perspectives on the issues under discussion.

This will take approx 20 minutes.

We will then ask all those present to form groups of 3-4, in the audience, to discuss the material presented and develop their own thinking in response.

The remainder of the session will be dedicated to short, snappy reports-back from participants on their stances on the issues.

A short wrap up by organisers at the end will summarise back the key themes heard.

Expected Outcomes: The outcomes will be
- a documented set of shared perspectives on the policy questions being discussed
- a broader understanding among all participants about the diversity of perspectives in answering the policy questions.

Discussion Facilitation:

The entire structure of the round table is interactive. By introducing topic material, and then having a short spontaneous breakout followed by report back, the audience will be encouraged to speak with people they do not know, share ideas in a low stress way, and share those perspectives back to the whole of the session.

Online Participation:

We will seek comments from those using the official tool and can read some into the record during the dialogue.

At least one speaker will be a remote participant and will contribute their views to the Round Table from the Pacific.

Proposed Additional Tools: We may make use of hashtags (to be agreed) on Twitter and other platforms in the lead up and during the round table, to elicit further input.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #148 International Cooperation on Cyber Threat Governance

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, Asia-Pacific Group
Organizer 4: Civil Society, Asia-Pacific Group

Speaker 1: Manuel Ifland, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Adli Wahid, Technical Community, Asia-Pacific Group
Speaker 3: Zhengxin WEI, Civil Society, Asia-Pacific Group

Policy Question(s):

1. What is the role of international cooperation in cyber threat governance? 2. What are the barriers to the international cooperation in cyber threat governance? 3. How should we cooperate with each other to tackle cyber threats? 4. What are the opportunities and challenges in dealing with cross-border cyber threats? 5. Are there any policies and strategies in place to provide guidance for such cooperation? 6. Are there any best practices in tacking cyber threats by cooperating with international partners?

Relevance to Theme: Nowadays, with the increasing emergence of cross-border cyber threats, cooperation across the whole world is keenly called for. One cannot stand alone and be immune in such an interconnected era. Such kind of international cooperation could help each concerned player well tackle cyber threats, improve resilience, raise security awareness and then facilitate the creation of a secure, safe, stable and resilient cyber environment.

Relevance to Internet Governance: As a non-government non-profit organization and representing the civil society, CNCERT/CC proposes this workshop with a view to enabling every stakeholder concerned to take this opportunity to share each other's experience and best practices to come up with some shared principles and programmes in tackling cyber threats through international cooperation, which will help achieve the secure and resilient development and use of the Internet, especially ICTs.

Format:

Round Table - U-shape - 60 Min

Description: This workshop mainly aims to facilitate information sharing and discussion among participants from governments, CERTs, renowned corporations, research institutions and academia worldwide to have an all-round engagement for each other to learn about and discuss experience and best practices related to international, public-private and private-private cooperation in tackling cyber threats and jointly push such international cooperation onto a higher and deeper level. This workshop will take place in a roundtable format, with the moderator introducing the invited speakers first, then each speaker delivering a short speech, and finally a fair amount of Q&A time from the floor. The questions that will be discussed during this workshop include but not limited to the role of international cooperation in cyber threat governance, barriers to such cooperation, the way to cooperate, the opportunities and challenges, related policies and strategies, and best practices.

Expected Outcomes: This workshop is expected to provide a face-to-face platform for concerned stakeholders to share and discuss each other's ideas and views, so as to find solutions and answer some major questions that are pertinent and raised in this area, help fulfill the requirements worldwide in addressing cyber threats of cross-border nature, and contribute to the creation of a secure, safe, stable and resilient cyber environment. We will also produce a summary report of this workshop and submit it to the IGF Secretariat within the required time limit.

Discussion Facilitation:

To effectively facilitate the discussion, we will first make sure that we have collected some demands from related parties through some informal discussions with our provisionally invited speakers, partners, and other concerned parties that are available in our resource pool. Second, based on the above research, we will well design some pre-set questions for the workshop to help everyone easily get engaged. Third, both the onsite and online moderators are experts in this area, who are familiar with the aim and mission of IGF, have a lot of experience in motivating the speakers and the audience, and possess the resourcefulness in handling all kinds of situations. Fourth, we will limit the speech time for each invited speaker for no more than 4 minutes and leave a fair amount of time for Q&A. Finally, we will fully and effectively use the online tool provided by IGF and Gotomeeting software (please refer to the "other tool" option for detailed information) to get more offsite audience engaged and enrich our discussion.

Online Participation:

Although this is the first time we apply for an IGF workshop, many colleagues in our organization have attended IGF meetings previously. We are aware of this platform and we will do full research on the use of

this tool from an organizer's perspective, get in touch with IGF for more information and get the right personnel from our side to make sure that we are both technically and procedurally prepared.

Proposed Additional Tools: APCERT, as the regional community for CERTs and CSIRTs located in the Asia Pacific region, provides online training for its members regularly through an online meeting tool called Gotomeeting. As an APCERT member, CNCERT/CC plans to use Gotomeeting to have APCERT members online to participate in this workshop and especially to actively engage in the Q&A session.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #150 Hacking Hate Speech Online: A multi-stakeholder approach

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
Hate Speech
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Intergovernmental Organization, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Hanna Gleiß, Civil Society, Western European and Others Group (WEOG)
Speaker 2: David NG, Civil Society, Asia-Pacific Group
Speaker 3: Sofia Rasgado, Government, Western European and Others Group (WEOG)
Speaker 4: Ricardo Campos, Government, Latin American and Caribbean Group (GRULAC)
Speaker 5: Sabine Frank , Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

- How can cooperation and collaboration on national, regional and global levels help to counteract hate speech online?

- How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and abuse in the online environment?

- How can their resilience be increased by means of capacity building, media literacy, support and guidance in the digital environment?

- What role should internet platforms play in defining the standards for acceptable content in light of freedom of speech?

Relevance to Theme: Online hate speech is a growing problem. People often experience the internet to be a hostile space. Hateful messages are increasingly common on social media. To complement existing

initiatives to regulate, monitor or report online hate speech, a more pro-active approach is needed to counteract hate speech online, building towards a secure, safe, stable and resilient internet environment.

Relevance to Internet Governance: Online hate speech can be identified as one of the growing threats to the global internet and its users. Hence, the urge to take an evidence-based approach to prevent and remediate online hate speech inevitable. Moreover, the importance of establishing a multi-stakeholder dialogue between governmental, civil society organisations and industry is key to strengthen shared principles, norms, rules and decision-making processes to fight hate speech online.

Format:

Break-out Group Discussions - Round Tables - 60 Min

Description: Hate speech is not a new phenomenon, it is as old as the formation of human societies and the organisation of people into groups. Defining the problem is the first challenge facing the speakers and participants of this session. In line with this, the session will table an academic literary review, highlighting conclusions from a range of countries and researchers on online hate to stimulate and inform the discussion.
Speakers will represent media regulators, civil society, policy makers, industry and of course youth will discuss and debate the issues and draw conclusions for the future of the internet governance agenda.

Intended agenda:
Opening by the moderator - What is at stake: Defining online hate speech (plenary - 15 min).
A multi-stakeholder approach - identifying strategies to counter hate speech (working groups lead by representatives from 1) government, 2) civil society, 3) industry and 4) youth - 30 min).
Sharing best practices to hack hate in the global internet - reporting back from 4 working groups (plenary 10 min).
Closing remarks and the way forward (plenary 5 min).

Expected Outcomes: During this session, participants will:

- Establish a common understanding on the definition of online hate speech.
- Identify strategies to counter online hate speech.
- Share examples of best practice (e.g. resources, local/global initiatives) in responding to online hate speech.

Discussion Facilitation:

In terms of format, the session will be organised as a facilitated dialogue. Led by the moderator, a diverse range of experts from different stakeholder groups - academia, government, industry, civil society and youth participation – will discuss key questions and issues. Possible questions may draw-upon:
What is online hate speech?
Which role can I/my organisation play in addressing online hate speech and changing society for the better?

In addition, each expert will facilitate a 30 minutes working group discussion in order to pro actively involve the whole audience. Each working group will identify strategies to counteract hate speech online which will be shared afterwards in plenary.

Furthermore, remote participation will be ensured through prior involvement of various stakeholders from across the world. The online moderator will ensure that remote participants are able to communicate questions to the onsite moderator during and after the debate.

Complementary to this, a social media campaign on Twitter will help to give further visibility to the session both prior, during and after the event. Live tweeting during the session will open the discussion to a wider online audience and will give remote participants the possibility to get directly involved in the debate.

Online Participation:

Remote participation will be ensured through prior involvement of various stakeholders from across the world. The online moderator will ensure that remote participants are able to communicate questions to the onsite moderator during and after the debate.

Proposed Additional Tools: Complementary to the online remote participation, a social media campaign on Twitter will help to give further visibility to the session both prior, during and after the event. Live tweeting during the session will open the discussion to a wider online audience and will give remote participants the possibility to get directly involved in the debate.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #151 Law enforcement online: Challenges for content regulators

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
FoE online
Hate Speech

Organizer 1: Government, Western European and Others Group (WEOG)
Organizer 2: Government, Western European and Others Group (WEOG)

Speaker 1: Kevin Bakhurst, Government, Western European and Others Group (WEOG)
Speaker 2: Tobias Schmid, Government, Western European and Others Group (WEOG)
Speaker 3: Marie-Teresa Weber, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

How should regulatory authorities with duties to regulate content in order to secure public policy objectives and safeguard compliance with core European values, approach the particular challenges presented by the increasing production and consumption of content via the internet?
How can the rights to freedom of expression be balanced by regulators against the potential harms from some types of content?
How can models of co-regulation and participatory regulation be employed, to harness the agility and expertise of internet actors, while giving sufficient confidence to regulators/policymakers and to the public?

Relevance to Theme: The regulatory and policy issues to be discussed form an important part of the broader set of issues around security and safety for internet users, in particular the safety of consumers and protection of minors using internet services.

Relevance to Internet Governance: Governments across the world, and in particular the national Governments of this session's participants, are currently developing principles and rules aimed at online

content regulation. This session will aim to inform that process, from the particular expert perspective of the experienced content regulator.

Format:

Birds of a Feather - Classroom - 60 Min

Description: Both Germany and the UK have seen recent developments and policy discussions around online content regulation. As the established broadcast regulators with responsibilities already extending to some areas of online content, the DLM and Ofcom have a unique expert perspective on these debates. National Regulatory Authorities across the EU and beyond have long been engaged in discussion around online regulation challenges, and the DLM and Ofcom have been active in those discussions, with Tobias Schmid, as Vice Chair of the European Regulators Group for Audiovisual Media Services (ERGA), currently leading work within that network.

This IGF presents a timely opportunity to continue those discussions with the benefit of broader participation from the multi-stakeholder community at the global level. The inclusion of the stakeholder's perspective, with a speaker joining us from Facebook, will enrich the discussion and provide a valuable technical and practical perspective.

The session will have a flexible agenda, since policy developments are in flux and it will be most useful to be able to respond to recent developments. But the intention is to discuss the challenges of online content regulation broadly, including the application of existing public policy goals and imperatives to new online paradigms of content creation and consumption. We anticipate drawing on thinking already done by the DLM and Ofcom, see background papers attached.

Expected Outcomes: To an extent the session is an end in itself: an opportunity to expose a wider set of stakeholders to some of the discussions between regulators that have been held privately or in more local fora over the past couple of years, and for the speakers to garner input from this community, and take it back to their respective organisations. But we anticipate also that expected outcomes could include follow-up initiatives between regulators, stakeholders and other participants, aimed at increasing mutual understanding, and furthering the achievement of public policy goals while respecting fundamental rights.

Discussion Facilitation:

The discussants will actively invite participation from other attendees.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: We plan to use Twitter to broadcast some key excerpts from the discussion and to invite comment.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 9: Industry, Innovation and Infrastructure
GOAL 12: Responsible Production and Consumption
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #152 Building Societal Resilience against Misinformation

Theme: Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Fake News
Trust and Accountability

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Technical Community, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Fabro Steibel, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Juliane von Reppert-Bismarck, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Lee Jennifer 8., Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

Worldwide there have been regulatory efforts to counter misinformation such as the 2017 Network Enforcement Act in Germany, the 2018 law against the manipulation of information in France, or the 2018 European Action Plan against disinformation. However, regulation faces at least three difficulties: 1. the danger of harming free speech and the free exchange of information online 2. the speed of technological development which makes it hard for regulation to keep up with and 3. the growing amount of misinformation distributed via encrypted messengers like WhatsApp and Telegram or fringe platforms such as Discord and Gab.ai, which are harder to regulate. Given these difficulties, it is increasingly important to complement regulation with broader efforts to empower citizens to use online information sources in a competent way and to foster societal resilience. The workshop will address the following policy questions:

Credibility indicators: How can we develop and implement more effective signaling mechanisms regarding the credibility of information online? What technological solutions do we need? What role is there for governments, technology companies, science, civil society and media?

Transparency: Which data do empowered users need from platforms to navigate modern information ecosystems? What kind of additional data sources should be available to ease the work of fact-checkers and to enable individuals to verify claims?

Digital and information literacy: What are the specific competencies citizens need to be able to identify false or misleading information online? How can these competencies be developed at scale on an individual (citizen) and organizational (civic society) level? What is the role for governments, technology companies, science, civil society and media?

Relevance to Theme: The increasing spread of misinformation has undermined trust in the internet as a foundation for the democratic, societal and economic participation of all citizens in a substantial way on a global scale. This workshop contributes to the topics of safety and resilience of internet users. Its goal is to identify key strategies to build up the capacity of citizens to distinguish between credible information and misinformation online. The workshop also takes into account the importance of a multidisciplinary perspective and stakeholder collaboration for responding to the growing threats to the global internet and its users. We see building societal resilience towards misinformation as a broad and long-term effort, which needs to engage governments, technology companies, academia and civil society, all of which are expected to present their views and contribute to the results of the workshop.

Relevance to Internet Governance: The question of how to build up societal resilience addresses the balance between freedom of expression on the internet and regulation to shield democratic systems from the negative effects of misinformation. A specific aim of the workshop is to identify rules, norms and mechanisms with the purpose of supporting citizens in their capacity to assess the credibility of online information. Thereby complementing public policy actions such as the action plan on disinformation by the European Union or the German Network Enforcement Act). Furthermore, the different roles and

responsibilities of government, civil society and the private sector for building societal resilience to misinformation will be a focus of the workshop.

Format:

Break-out Group Discussions - Flexible Seating - 90 Min

Description: The organizers believe that strengthening societal resilience and empowering the individual to assess the credibility of information online is necessary to guide regulatory responses to misinformation. The workshop at the IGF will be following a multidisciplinary roundtable hosted by the Oxford Internet Institute and the Vodafone Germany Foundation in Berlin in March 2019. The roundtable generated several preliminary ideas for building resilience towards misinformation with a focus on the European Union. With the workshop at the IGF we would like to continue the discussion with a wider range of stakeholders and with a more international perspective.

Preliminary Workshop Agenda:

Setting the Scene: why focus on societal resilience with regard to misinformation?
Input by Lisa-Maria Neudert, Oxford Internet Institute (20 min.)

Breakout Sessions (40 min)
1. Credibility indicators
- Input by Jennifer 8. Lee, Credibility Coalition (10 min): What are current examples and technological possibilities?
- Discussion: What is needed in addition?
- Discussion: What can Governments, Civil Society, Academia and the private sector do to develop more/better credibility indicators?

2. Transparency
Input by Fabro Steibel, ITS Rio (10 min): Recent developments in platform transparency
- Discussion: What kind of context information should be available on platforms and in what way/format to be accessible for the individual user?
- Discussion: What kind of additional data sources are needed to support the work of fact checkers and to enable individuals to verify claims?

3. Digital and information literacy
Input by Juliane von Reppert-Bismarck, lie-detectors (10 min): What are basic competencies to assess the credibility of online-information?
- Discussion: How can these competencies be developed in the citizenry at scale?
- Discussion: What role is there for governments, civil society, education and the media?

Presenting the results of the breakout sessions (30 min)
Each group will have 5 minutes to present their results and 5 minutes to answer questions.

Each breakout group will be moderated by a member of the organizing team or one of the speakers. The results of the discussion should be visualized (whiteboard, sticky notes etc.). The members of the breakout sessions should choose a rapporteur amongst themselves to present the results of the discussion in the plenary.

Expected Outcomes: The purpose of the workshop is to generate ideas on societal resilience towards misinformation from great variety of stakeholders and geographical representations. These ideas can address the three policy questions addressed by the workshop but are not limited to them. We expect concrete outcomes of the workshop on two levels:
- Building blocks for a strategy to build up societal resilience towards misinformation
- Identifying and connecting Individuals and organizations who are willing to further develop recommendations and policy proposals.

We will summarize the outcomes of the workshop in a working paper and distribute a draft of the paper to the participants for comments before publishing it. Furthermore, the organizers plan to continue the dialogue on societal resilience towards misinformation with civil society organizations and other stakeholders with the aim of publishing concrete recommendations and policy proposals.

We aim to collaborate with other workshop organizers in the same field to ensure that our session is complementary and to drive collaboration in this space beyond the IGF.

Discussion Facilitation:

A principal aim of the workshop is to generate an open discussion and to assemble as much input from diverse perspectives on societal resilience towards misinformation as possible. The format of the breakout sessions was chosen to facilitate parallel discussions and to enable individuals to present their views and ideas in a smaller group setting.

Online Participation:

The moderator for the workshop as well as the moderators for the three breakout sessions will feed points made or questions asked within the online participation tool into the discussion.

SDGs:

GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #154 How Children's Rights help us to a safe and global Internet

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Child Online Safety
Human Rights
Internet ethics

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Gehad Madi, Intergovernmental Organization, African Group
Speaker 2: AMANDA THIRD, Technical Community, Asia-Pacific Group
Speaker 3: Sonia Livingstone, Technical Community, Western European and Others Group (WEOG)
Speaker 4: Nomshado Lubisi, Civil Society, African Group

Policy Question(s):

Why are children's rights essential in the digital environment?
What is necessary for the implementation of children's rights in the digital world?
What does a General Comment on Children's Rights in relation to the digital environment mean to State parties and Governments?
What responsibility do society, politics and business have for a good and safe growing up with media?
What importance do children themselves attach to a human rights-based, secure and global Internet?

Relevance to Theme: Information and communication technologies (ICTs) have become an integral part of children's lives. The Internet offers children a wide range of opportunities, but also exposes them to a number of risks. Both, online opportunities and online risks have to be taken into account when considering the United Nation's Convention on the Rights of the Child. Children's rights also need to be respected, protected and fulfilled in the digital environment, which is a key challenge to society, politics and economics in the 21st century. The child rights perspective opens the view on both the possibilities and the necessities of how children can be kept safe online.

Relevance to Internet Governance: The important discourse on digital children's rights is currently still taking place in a niche and taking into account the children's rights perspective when it comes to Internet Governance is still an underrepresented approach worldwide. At the same time, the UN Convention on the Rights of the Child has been adopted since 30 years and must finally be applied to all areas of life - offline and online - and be reflected in government measures as well as in the actions of the private sector and civil society. Thus it is possible to develop a human rights based, safe and global internet. The importance of this step is underlined by the work of the UN Children's Rights Committee on the General Comment on Children's Rights in relation to the digital environment.

Format:

Panel - Auditorium - 90 Min

Description: The panel wants to inform about the vision and the very new process of developing the General Comment on Children's Rights in relation to the digital environment. Stakeholders of this process are invited to report in keynotes about their institution (i.e. the UN-Committee on the Rights of the Child), their expectations and challenges. Inputs from the speakers bring light into the valuable work of children's rights in digital contexts.
This leads to the title question, how children's rights can help us to a human rights based, safe and global Internet. The panel plans to discuss, which children's rights are mainly affected, what are controversy issues to stakeholders and state parties and how are children's views, interests and experiences implemented in the development of the General Comment.

Expected Outcomes: - Understanding of the importance and chances of children's rights in the digital environment and the relevance to state parties and other stakeholders
- Learning about the collaborating process of developing a General Comment including the views of different experts from diverse geographical, cultural, political and business regions
- Learning views of children and youth including in the draft of the General Comment

Discussion Facilitation:

We will inform people from our diverse network about the date and topic and policy questions of our workshop, that they are able to participate personally or online to bring in their perspective and questions. Our network includes persons from all different stakeholder groups in different countries, governmental, technical community, private sector, civil society, youth experts.

Online Participation:

We will inform people from our diverse network about the date and topic and policy questions of our workshop, that they are able to participate online and to bring in their perspective and questions.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption

IGF 2019 WS #155 Anywhere: Security of IoT Devices

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, Asia-Pacific Group
Organizer 4: Civil Society, Asia-Pacific Group

Speaker 1: Denis Legezo, Private Sector, Eastern European Group
Speaker 2: Noelle Francesca de Guzman, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Abel Torres, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

1. What is the current status of the security of IoT devices in your constituency? 2. Have you experienced any real cases? 3. What solutions are available in your entity? 4. What are the opportunities and challenges regarding the security of IoT devices? 5. Are there any policies and strategies in place to provide guidance for this area? 6. What are the roles of concerned parties and how can they cooperate with each other?

Relevance to Theme: As the emerging technologies advance, our physical world is becoming more Internet-enabled where various kinds of devices, vehicles, buildings and other items are connected to collect and exchange data. While bringing tremendous benefits to people's lives, such Internet of Things (IoT) has also led to the increasing emergence of new cyber threats and incidents, exerting huge socio-economic impact on every economy and affecting the security, safety and stability of the world.

Relevance to Internet Governance: CNCERT/CC, as a non-government non-profit organization and representing the civil society, hopes that through this workshop, every stakeholder concerned can take this opportunity to share each other's experience and best practices to lay down some shared principles and find some possible solutions regarding the security of IoT devices, which will help shape the development and use of the Internet.

Format:
Birds of a Feather - Classroom - 60 Min

Description: This workshop touches upon a hot topic in the current interconnected era with not only people connected, but also things. It mainly aims to facilitate experience sharing, solution finding and discussion among participants from international organizations, governments, CERTs, renowned equipment manufacturers, and software providers worldwide to shed some lights on the current security situation of IoT devices, government strategies, technical solutions and best industrial practices, so as to raise everyone's awareness and improve protection skills. This workshop is expected to be carried out in a Birds of a Feather format, with short speeches by each invited speaker and discussion for the rest of the session. We will set the tone of this workshop by providing some commonly concerned topics, such as the status quo, policies or guidelines, technical approaches, industrial countermeasures, challenges and ways forward, to get everyone easily engaged and also leave out a lot of free discussion time for everyone to share their experience and comments. The questions that will be discussed during this workshop include but not limited to the current status of the security of IoT device, case studies, available solutions, opportunities and challenges, policies or strategies, roles of concerned parties, and way to cooperate.

Expected Outcomes: We expect to find some possible solutions and some interesting perspectives concerning the security issue of IoT devices through this workshop by looking at this issue in a full-dimensional manner. On the one hand, this workshop will enlighten each participant with up-to-date statistics, policy suggestions, innovative technical approaches and guidelines that may not be easily and intensively acquired through other means; on the other hand, it will also inspire the participants with perspectives and experiences which could be well adapted and incorporated into their own conditions, so as to jointly build a secure, safe, stable and resilient environment. After the workshop, a summary report will also be produced and submitted to the IGT Secretariat within the required time limit.

Discussion Facilitation:

To effectively facilitate the discussion, we will first provide some pre-set questions which are designed based on both our own experience and concerns collected from related parties. Then, we will provide a fair amount of time for discussion, both on pre-set topics and in a free manner, to ensure that the whole audience will actively engage in and provide some fresh ideas and comments apart from our invited speakers. Third, we will make sure that the whole session will be efficiently and smartly moderated by our experienced moderator/expert to get the whole event lively and focused. Fourth, we will limit the speech time for each invited speaker for no more than 4 minutes and leave a fair amount of time for discussion. Finally, we will fully and effectively use the online tool provided by IGF and Gotomeeting software (please refer to the "other tool" option for detailed information) to get more offsite audience engaged and enrich our discussion.

Online Participation:

Although this is the first time we apply for an IGF workshop, many colleagues in our organization have attended IGF meetings previously. We are aware of this platform and we will do full research on the use of this tool from an organizer's perspective, get in touch with IGF for more information and get the right personnel from our side to make sure that we are both technically and procedurally prepared.

Proposed Additional Tools: APCERT, as the regional community for CERTs and CSIRTs located in the Asia Pacific region, provides online training for its members every two months through a online meeting tool called Gotomeeting. As an APCERT member, CNCERT/CC plans to use Gotomeeting to have APCERT members online to participate in this workshop and especially to actively engage in the Q&A session.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #157 New Methods for Social Media Monitoring during Election

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
Hate Speech
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Intergovernmental Organization, Intergovernmental Organization

Speaker 1: Ramali Khadeja, Civil Society, African Group
Speaker 2: Rafael Schmuziger Goldzweig, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Giovanna Maiola, Intergovernmental Organization, Western European and Others Group (WEOG)

Policy Question(s):

What are the existing methodologies to usefully monitor political campaigns ahead of elections?
How much has social media monitoring been able to assess the integrity of electoral processes?
What aspects of social media do we need to consider before designing a strategy to monitor disinformation?
What can be done to turn social media into more democratic spaces and free of manipulation from extreme groups and foreign actors?
Beyond election campaigns and hate speech monitoring, what are the other possible uses of social media monitoring to ensure the integrity of public discourse?

Relevance to Theme: Social media have transformed public discourse and political debate. Some NGOs have started monitoring social media in elections: in 2018, there has been a flurry of new social media monitoring initiatives around various elections. 'Supporting Democracy', a technical assistance project of the European Commission (DG International Development and Cooperation) has set up a working group on social media monitoring with two of its member organizations: Democracy Reporting International (Germany) and the National Democratic Institute (US) and various CSOs worldwide such as ISFED (Georgia), DRF (Pakistan), etc.
Monitoring the threats and improving the political discourse online is key in order to increase resilience of democratic institutions and safeguard voters' prerogative to exercise their political rights without being manipulated. This session will present and discuss the working group's findings. In particular, it will compare the pros and cons of various methodologies that civic groups have tested in various countries and how a joint methodology can help future attempts to identify hate speech, information operations, and others. The roundtable aims to sketch out possible plans for larger cooperation among civil society groups that wish to monitor social media in elections, and within the broader agenda of monitoring the integrity of public discourse.

Relevance to Internet Governance: Dealing with the threats associated with social media use around elections is far too complex to be done by just one stakeholder. When it comes to tackling information operations on social media platforms that aim to discredit a candidate, spread conspiracy theories and false information, and to polarise people's opinions, one should consider not only state regulation, but also through a change in the design of social media platforms. Civil society groups can play a central role in this fledgling debate, as they have been gathering evidence through diverse methodological approaches over the past few years and can claim to be the best positioned to usefully contribute to this debate. Our roundtable will discuss which directions stakeholders in social media monitoring may explore in order to turn social media into a healthier, more credible democratic space for political confrontation and debate.

Format:
Round Table - U-shape - 90 Min

Description: With the rise of social media, electoral campaigns have been increasingly subjected to political manipulation through false information, hate speech, and coordinated campaigns against minorities. Together, Democracy Reporting International (DRI) and the National Democratic Institute (NDI) have been working on a methodology to monitor social media during electoral cycles and beyond. In so doing, they also intend to make a useful contribution to updating the capacity of international Election Observation Missions that ensure that democratic processes are credible, and that rules are respected both online and offline. Under the Supporting Democracy initiative, they have been testing and improving their new methodologies for social media monitoring in direct cooperation with local civil society organisations such diverse countries as Georgia, Lebanon, Pakistan and Thailand.

In 2018, based on its pioneering work of monitoring social media ahead of the 2017 German general elections, DRI published a paper that charted an approach towards a social media monitoring methodology. They also published a report on disinformation, international law, and election observation. Supporting Democracy successfully organised the EU's first global campaign on civic technologies for democracy, 'CivicTech4Democracy' in the same year, and launched a global study on 'Innovative Approaches to Citizen Participation in Restrictive Environments' which examines how civil society can bypass authoritarian restrictions to election observation through remote social media-based elections analysis. This session will mobilise IGF participants on these topics and will discuss options for international cooperation, based on 'open source' sharing of successful solutions and tools.
This session intends to spark interest and draw attention to the various ways in which social media monitoring can be designed and implemented. It aims to pave the way for broad cooperation mechanisms among civic groups across the world on shared design principles.
Based on this expertise, we propose the following outline:
a. Intro with key aspects of the methodology
b. Findings from different countries (we will define which cases are more important from the analysis we performed/will perform in Sri Lanka, Pakistan, Libya, Tunisia, Nigeria, Germany, Brazil).
c. Address the existing challenges in social media monitoring during elections. How can this exercise be improved? what are the role of companies in that effort? how can Observation Missions be more attentive to the online environment?

Expected Outcomes: • Increase awareness among Civil Society Organisations and point out to best practices that will support them in their monitoring efforts.
• Spark a debate about what companies can do to improve the design of their products, changing the incentives of malicious actors to engage in information operations and hate speech in the context of elections
• Define routes that policy makers can explore when it comes to regulation: what are areas where regulation is desirable, and which fields regulation may be ineffective?

Discussion Facilitation:

Since it's a methodology, we aim at giving short inputs and results to make the discussion more concrete. We will have short sessions of discussions divided in three topic areas around election observation (monitoring paid ads, monitoring hate speech and monitoring disinformation) welcoming inputs from the participants.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: Show some aspects of the methodology on slides, potential findings and points for discussion. (projector, presentations)

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #159 Towards a Human Rights-Centered Cybersecurity Training

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

Capacity Building
Cyber Security Best Practice
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: caroline sinders, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Farhan Janjua, Civil Society, Asia-Pacific Group
Speaker 3: Adli Wahid, Technical Community, Asia-Pacific Group
Speaker 4: Chris Kubecka, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

What role should different stakeholders play in cybersecurity capacity building approaches? How can resilience and security of cyberspace be increased by means of capacity building, media literacy, support and guidance in the digital environment? How can consumer rights and consumers' capacity to protect themselves and their data be reinforced?

(please see agenda for more specific policy questions to be discussed in the session)

Relevance to Theme: In this workshop we want to put the focus on security and safety via cyber security of the people. Cybersecurity training should increase the capacity of citizens to become more secure online and therefore demand and defend their human rights safely if the state should infringe upon them. This workshop will take this aim. Furthermore, capacity building and collaboration with diverse stakeholders can ensure that users achieve certain levels of digital and legal literacy, so that if state practices infringe upon their rights and threaten individual security, there is recourse. A human rights centred approach to cybersecurity training is necessary so that vulnerable groups and minorities can benefit from access to technology and the infrastructure with which their state provides them.

We are therefore asking in this workshop:
How can we create cybersecurity trainings that aim to save these communities when principles of human-rights based cybersecurity fail? How can we properly ensure that programs that build cybersecurity capacity are actually human-rights based? Furthermore, how can these rights be operationalized in capacity-building programs for vulnerable groups through cybersecurity trainings?

We will evaluate different roles of stakeholders and cybersecurity training set-up to gather best practices on achieving a human rights-centred approach to cybersecurity training that is sustainable at all levels of society - from the state to the individual. Here we specifically also want to include stakeholders that are usually involved in building capacity for cybersecurity and resilience of a state actor, such as Computer Emergency Response Teams asking what could their role be in achieving the same for citizens? Moreover, we want to connect stakeholders that are involved in capacity building programs and those who work on human rights and/or are affected by state actions against human rights and need cybersecurity training to protect themselves.

Relevance to Internet Governance: While recommendations on how to have a human rights-based cybersecurity policy, were spelled out IGF in 2018 ("The development of cybersecurity-related laws, policies, and practices should from their inception be human rights-respecting by design."), this does not mean that states necessarily take this into consideration when crafting their cybersecurity practices. The issue of cybersecurity has been prioritized at the state level to protect national security. The focus on the state and "its" security crowds out consideration for the security of the individual citizen, not least because in some areas of the world, it has become the case that more security means infringing upon individual freedoms

and liberties, by means of government hacking for example. The type of security that is currently prioritized is often not security (directly) relevant to the people --- examples that this is the case: Repressive laws, increased surveillance, and regulatory controls from governments such as China, Egypt, the United Kingdom, Canada, Germany and France have also increased. Additionally, calls to ban security and anonymizing tools such as Tor have come from Russia, Pakistan, Belarus, and was recently also called for at the European police congress. These varied policies and practices are changing the nature of the Internet and creating challenges regarding its technical and legal fragmentation

Format:

Other - 90 Min
Format description: "World Cafe" Format: Three tables for (rotating) group discussion, flip board at each table, online participation provided by online document and video conferencing, moderators will wrap-up group discussions while participants can enter contributions and thoughts into the online document.

Description: "World Cafe" format: Different tables with different themes - this will encourage diverse conversations, exchange of diverse perspectives, and allows for flexible and inclusive discussion.

Brief input from journalist,"Why I needed cybersecurity training"

Intro to World Cafe on "Gathering best practices to human rights centered cybersecurity trainings"

Rotating - Three rounds for gathering best practices on human rights centred cybersecurity training at different tables. Each round is 20 minutes, before the start of the rounds, moderators will summarize the discussions and work of the previous round. Participants are free to rotate to different tables or stay at one table the whole time. The themes of the three tables are as following:

Table 1: Focus on roles of stakeholders (at this table, the goal is to understand how different stakeholders can take a human rights-centered approach to cybersecurity training. For specific input as well as policy questions to be discussed, see "Agenda and Methodology" attached as PDF)

Table 2: Focus on human rights-centered IT-security solutions that are needed in cybersecurity training (at this table, we will discuss which IT-security solutions are needed in cybersecurity trainings and can be promoted as human rights-centered, and ultimately raise capacity of vulnerable groups. For specific input as well as policy questions to be discussed, see "Agenda and Methodology" attached as PDF)

Table 3: Focus on overcoming challenges to human rights-centered cybersecurity training (at this table, a journalist from Pakistan will share anecdotal evidence for why cybersecurity trainings need to consider human rights at their core and how challenges to such cybersecurity trainings can be met. For specific input as well as policy questions to be discussed, see "Agenda and Methodology" attached as PDF)

Wrap-up discussion by moderators and summary of table discussion.

For more detailed agenda and methodolgy, please see "Agenda and Methodology" attached as PDF in Additional Documents.

Expected Outcomes: - Some best practices of achieving sustainable human rights centered cybersecurity training for vulnerable groups
- A better understanding of what human rights centered capacity building means for different stakeholders and their responsibility for implementation
- Putting the focus on security and safety via cybersecurity of the people by shifting away from solely looking at "national" security of the states, which sometimes violates security and safety of the citizens

Discussion Facilitation:

We will be present at the different tables and encourage discussion and inclusion, so that the speakers have the forum to discuss what they, as practitioners, think is crucial. We will also moderate the online discussion

and make sure the online document is kept up-to-date during discussion for transparency and increased inclusion.

Online Participation:

To gather input and contributions from online participants throughout the session. Both a document to gather thoughts and be transparent about ongoing discussion, as well as video conference tools to allow for remote participation.

Proposed Additional Tools: Flipcharts, post-its, and online document to engage participants in different means so that it is not just round-table discussions.

SDGs:

GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Background Paper

IGF 2019 WS #165 Round Table on Cyberlaw, Cybercrime & Cybersecurity

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
International Norms
Cyber Crime

Organizer 1: Private Sector, Asia-Pacific Group

Speaker 1: PAVAN DUGGAL, Private Sector, Asia-Pacific Group
Speaker 2: Alfredo RONCHI, Civil Society, Western European and Others Group (WEOG)
Speaker 3: CHRISTOPH STUECKELBERGER, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

The policy questions for the Round Table on Cyberlaw, Cybercrime & Cybersecurity are as follows:-

1. What should be the approaches that the global stakeholders need to adopt in the context of Cyberlaw, Cybercrime & Cybersecurity?

2. What are the current challenges which require urgent attention of national governments and regulators in cyberspace?

3. How can the issue of cyber security breaches be appropriately addressed by various state and non-state actors ,given the challenges of attribution and jurisdiction in cyberspace

4. How can the international cooperation be enhanced in the context of cyberspace and in the context of cyber security and Cyberlaw?

Relevance to Theme: The Round Table on Cyberlaw, Cybercrime & Cybersecurity is a unique concept that is devised, hosted and implemented by Pavan Duggal Associates, Advocates led by Dr. Pavan Duggal, Advocate, Supreme Court of India, an internationally renowned expert and authority on Cyberlaw and Cybersecurity and one of the top four cyber lawyers in the world.

The Round Table on Cyberlaw, Cybercrime & Cybersecurity is based on an interactive format wherein the cutting-edge developments concerning Cyberlaw, Cybercrime & Cybersecurity as also emerging technologies on Cyberspace are appropriately discussed and debated with the regional and national governments, officials, corporates, academia and other respective stakeholders.

The said Round Table could examine the cutting-edge issues concerning Cyberlaw, Cybercrime & Cybersecurity and give details about the cutting-edge challenges that the cyber ecosystem is facing and thereafter further discuss as to how these challenges are being addressed by different countries with varioua respective national stakeholders and thought leaders and heads of appropriate governmental departments. It may take into consideration the particular requirements and consideration of the IGF and also how national strategies could be appropriately informed by intelligent decision making, taking into account the relevant parameters concerning Cyberlaw, Cybercrime & Cybersecurity being discussed at the Round Table.

The deliberations of Round Table on Cyberlaw, Cybercrime & Cybersecurity could further be fed into the consultations and deliberations of International Conference on Cyberlaw, Cybercrime & Cybersecurity which is an annual event on Cyberlaw, Cybercrime & Cybersecurity.

Relevance to Internet Governance: The relevance of Round Table on Cyberlaw, Cybercrime & Cybersecurity to Internet Governance is very topical. For Internet to be governed, it is imperative that Internet must be robust, secure, resilient and reliable. For that, various issues pertaining to cyber security need to be appropriately addressed. This Round Table will seek to address important issues concerning cyber security that need to be addressed in order to make Internet Governance more pertinent and relevant.

Further from the perspective of norms of behavior in cyberspace, it is imperative that appropriate Cyberlaw frameworks and jurisprudence must be effectively evolved. In that regard, it must be essential that Internet Governance would be likely benefited by the emerging discussion on Cyberlaw jurisprudence which could have a direct effect upon Internet Governance.

Since cybercrime is growing at a very rapid pace, it is very essential and imperative that there must be now more cogent and better ways of tackling cybercrimes given the advent of Artificial Intelligence, Internet of Things and Blockchains and also the darknet. This Round Table will seek to identify some key strategies that need to be adopted by state and non-state actors in this regard as they go forward.

Format:

Round Table - Circle - 90 Min

Description: The Round Table on Cyberlaw, Cybercrime & Cybersecurity is based on unique interactive format wherein the cutting-edge developments concerning Cyberlaw, Cybercrime & Cybersecurity as also emerging technologies on Cyberspace are appropriately discussed and debated with the regional and national governments, officials, corporates, academia and other respective stakeholders.

The said Round Table could examine the cutting-edge issues concerning Cyberlaw, Cybercrime & Cybersecurity. The Round Table would inform the discussions at the International Conference on Cyberlaw, Cybercrime & Cybersecurity, 2019 to give details about the Outcome Document and further give details about the cutting-edge challenges that countries across the world are facing.

Expected Outcomes: The deliberations of Round Table on Cyberlaw, Cybercrime & Cybersecurity could further be fed into the consultations and deliberations of International Conference on Cyberlaw, Cybercrime & Cybersecurity, 2020 which will take place in New Delhi in November, 2020.

Discussion Facilitation:

It will be an interactive Round Table discussion format where there will be no presentations. However, the Moderator will call upon individual stakeholders to contribute in an interactive manner.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #167 Artificial Intelligence, Law, Ethics & Emerging Challenges

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Human Rights
Internet ethics

Organizer 1: Private Sector, Asia-Pacific Group

Speaker 1: PAVAN DUGGAL, Private Sector, Asia-Pacific Group
Speaker 2: CHRISTOPH STUECKELBERGER, Civil Society, Western European and Others Group (WEOG)
Speaker 3: SALMA ABASSI, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

1. Artificial Intelligence is growing at a very rapid pace. However, how does it need to be regulated at international level?

2. Is there a need for providing legal recognition to Artificial Intelligence?

3. Can the ethical dimensions of the acts done by Artificial Intelligence be appropriately addressed by ethical and legal frameworks?

4. How can cybercrime connected through Artificial Intelligence thus be regulated?

5. How can the issue of misuse and breach of cyber security by Artificial Intelligence be appropriately addressed?

These and other important policy questions are likely to be raised by the present Workshop. The Workshop will also look at how the advent of Artificial Intelligence law and legal frameworks are having an impact upon the way how Artificial Intelligence jurisprudence is evolving.

Relevance to Theme: Artificial Intelligence has gained lot of centre-stage attention. Lot of cutting-edge developments are taking place in Artificial Intelligence. These developments have compelled the need for giving appropriate attention to the legal and policy challenges raised by Artificial Intelligence. Further, the ethical ramifications of Artificial Intelligence is increasingly getting more and more significant. It is imperative to ensure ethical behaviour standards for Artificial Intelligence.

This Workshop will examine the legal emerging challenges that Artificial Intelligence has thrown up and would also examine how different approaches at global level are trying to address the other legal challenges. Further, the ethical ramifications of Artificial Intelligence need to be appropriately addressed given the documented instances where Artificial Intelligence algorithms have demonstrated bias based on the big data sets that are fed therein. This workshop will also examine the ethical ramifications of Artificial Intelligence and how the same need to be addressed. It will further examine how the frameworks in this regard are evolving at global level which further would necessitate far more action.

Relevance to Internet Governance: The present Workshop on Artificial Intelligence has a direct relevance to Internet Governance. Today, for Internet to be properly governed, it must be taken into account the newly emerging technologies like Artificial Intelligence. Artificial Intelligence can also provide more effective, practical and conducive ways for governing Internet in a right direction. The Workshop will try to explore some of the key areas or connection between Artificial Intelligence and Internet Governance and how Artificial Intelligence could be potentially harnessed for the purposes of better Internet Governance.

Format:

Round Table - U-shape - 90 Min

Description: Artificial Intelligence has gained lot of centre-stage attention. Lot of cutting-edge developments are taking place in Artificial Intelligence. These developments have compelled the need for giving appropriate attention to the legal and policy challenges raised by Artificial Intelligence. Further, the ethical ramifications of Artificial Intelligence is increasingly getting more and more significant. It is imperative to ensure ethical behaviour standards for Artificial Intelligence.

This Workshop will examine the legal emerging challenges that Artificial Intelligence has thrown up and would also examine how different approaches at global level are trying to address the other legal challenges. Further, the ethical ramifications of Artificial Intelligence need to be appropriately addressed given the documented instances where Artificial Intelligence algorithms have demonstrated bias based on the big data sets that are fed therein. This workshop will also examine the ethical ramifications of Artificial Intelligence and how the same need to be addressed. It will further examine how the frameworks in this regard are evolving at global level which further would necessitate far more action.

The Workshop would be organized by Artificial Intelligence Law Hub which is world's unique Hub looking at cutting-edge legal principles governing Artificial Intelligence.

Expected Outcomes: The workshop will aim to suggest practical approaches on how to deal with the emerging legal and ethical issues concerning artificial intelligence today.

Discussion Facilitation:

The workshop will be in an interactive format. The workshop will encourage more participation from participants and also various stakeholders from different sectors and corners.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #168 Cyber Sovereignty & Cyber Security Law

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Private Sector, Asia-Pacific Group

Speaker 1: PAVAN DUGGAL, Private Sector, Asia-Pacific Group
Speaker 2: CHRISTOPH STUECKELBERGER, Civil Society, Western European and Others Group (WEOG)
Speaker 3: SALMA ABASSI, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

1. What is the concept of cyber sovereignty? What are its limits?

2. How are countries trying to expand the scope of cyber sovereignty using cyber security regulation?

3. What is the actual implementation capability of such provisions concerning cyber sovereignty?

4. Does Internet jurisdiction not pose a challenge to cyber sovereignty?

5. What can be the limits for cyber sovereignty?

6. Could the cyber sovereignty of one country potentially be violating or contravening the cyber sovereignty of another country/

7. How can the cyber sovereignty of different countries be appropriately balanced by putting in adequate limits?

8. What is the legal framework in the event if there is a breach of cyber sovereignty of one country by other countries?

9. What is the international mechanism in the event there is a dispute between different countries to the extent of applicability and expanse of cyber sovereignty of countries?

These and other policy questions are likely to be discussed in the proposed Workshop.

Relevance to Theme: Today different countries are coming up with different national legislation on cyber sovereignty. One of the key thrust areas of the said legislation is cyber sovereignty. Different countries are expanding their scope and applicability of cyber sovereignty. This workshop will look at how cyber sovereignty as a concept has evolved and how cyber security law has been evolving as an instrument for further enhancing the cyber sovereignty of different countries.

This workshop will look at the role of cyber sovereignty in enhancing the cyber security law jurisprudence.

The proposed workshop will be organized by International Commission on Cyber Security Law.

Relevance to Internet Governance:
Cyber sovereignty has a direct relevance to Internet Governance. Internet Governance today is going through very transient times. The norms of behavior in cyberspace have not been appropriately developed. On top of it, different national legislations are coming up with different national perspectives and visions of what is cyber sovereignty. Very expansive definition of cyber sovereignty is currently being given so as to expand the applicability and ambit of national laws to areas beyond the territorial boundaries of different countries.

In a scenario like this, the proposed Workshop will try to examine the interconnection between cyber sovereignty, cyber security law and the Internet Governance. The broader the countries are defining their concepts of cyber sovereignty, the higher the chances that it could have potential prejudicial impact upon the entire issue of Internet Governance. For the purposes of governing the entire Internet properly, more holistic and balanced approaches need to be adopted in the context of cyber sovereignty.

Further, Internet Governance mechanisms must provide for adequate and efficacious adjudication of disputes between countries pertaining to the extent of the cyber sovereignty. These and other important issues in cyber security law have a direct connection on Internet Governance. As such, the present Workshop will be extremely relevant from the perspectives of both state and non-state actors. The proposed workshop will deliberate as to how appropriate norms could be developed so as to provide to the world, a balanced approach on cyber sovereignty, in order to minimize potential disputes between nations and in order to provide more harmonious coexistence so that Internet Governance can be effectively implemented in a far more efficacious harmonious and constructive manner

Format:
Round Table - Circle - 90 Min

Description: Today different countries are coming up with different national legislation on cyber sovereignty. One of the key thrust areas of the said legislation is cyber sovereignty. Different countries are expanding their scope and applicability of cyber sovereignty. This workshop will look at how cyber sovereignty as a concept has evolved and how cyber security law has been evolving as an instrument for further enhancing the cyber sovereignty.

This workshop will look at the role of cyber sovereignty in enhancing the cyber security law jurisprudence.

The proposed workshop will be organized by International Commission on Cyber Security Law.

Expected Outcomes: The workshop will aim to come up with potential solutions and approaches that could be adopted in order to minimize potential confrontation between different nations , in the event of conflicts arising concerning cyber sovereignty of nations.

Discussion Facilitation:

The workshop will be in an interactive format. The workshop will encourage more participation from participants and also various stakeholders from different sectors and corners.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #170 Children's Privacy and data protection in digital contexts

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):

Child Online Safety
Human Rights
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Steffen Eisentraut, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Sonia Livingstone, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Phakamile Phakamile, Civil Society, African Group

Policy Question(s):

What are the views and positions of different stakeholders on children's rights to privacy and data protection?
Who is responsible for the protection of data of children and how to fill the gaps of implementation?
How to responsibly balance between protection and participation rights of children?

Relevance to Theme: Personal rights such as the right to privacy and honour are not new. However, they become particularly relevant in the context of digital media use and digitisation. In view of the rapid and diverse distribution channels, personal data such as images or personal data in various forms like location or interests can quickly get out of control of one's own sphere of action and cause lasting damage. Especially when it comes to children and young people being online and becoming consumers of products and services, a particularly high responsibility to protect their privacy at various institutional levels is justified. These stakeholders must develop appropriate strategies that correspond and work together. Individuals, families, educational institutions and the state, and especially providers and developers of technologies, algorithms, games and online services, have to put personal rights before particular interests. These stakeholders are well aware of the many risks of media use and their responsibility towards children. However, their practice and actions often contradict this. There is a need for understanding and action here.

Relevance to Internet Governance: Child safety online is an essential issue worldwide. States have a special role of responsibility when it comes to the personal rights of their citizens, especially their children. They regulate how effectively data protection and privacy are respected and realised in their countries, how valuable and dignified the personality of each individual is respected on a legal level, social level as well as on the individual level. As contracting states to the UN Convention on the Rights of the Child, their actions and designs must correspond to the right of children to privacy and honour in accordance with Art. 16 of the Convention, also in the digital sphere.

Format:

Break-out Group Discussions - Flexible Seating - 90 Min

Description: The session will start with a brief moderated discussion of five different experts that will introduce their specific point of view. The participants are then invited to form five teams and each team is joined by one of the experts. The break out group discussion will be divided into five rounds of 10 minutes each. After every 10 minutes the experts leave their team and join a different team. That way each participant has the chance to intensely discuss with all the experts.
For the discussion rounds we will provide questions and hypotheses to start and guide the discussion. Furthermore we will provide templates to structurally document the main aspects and outcomes of each discussion round. After each round the templates will be collected, clustered and displayed on a wall by the organizers. After the 5 break-out sessions the participants are invited to review the outcomes of each round at presentation wall. The session will close with a guided discussion about the learnings and outcomes.
Agenda Outline
1. Experts Input (15 min)
2. Break-Out Session (50 min)
3. Presentation Wall (15 min)

4. Reflection and Discussion (10 min)
Expert topics
1. Governmental regulation: Possibilities and instruments of monitoring violations of children's privacy online
2. Digital Parenting. Privacy online and data protection in the context of the family
3. Education and media literacy: How to empower children and young people to become self-determined media users who respect human rights and privacy online
4. Technical Community – How engineers of Apps, games, platforms and devices can contribute responsibly to protect children's data and privacy
5. Civil Society/NGO – A child rights perspective on privacy online and data protection for children and young people

Expected Outcomes: - Understanding of controversy perspectives on children's privacy online
- Raising awareness on risks of violation of children's privacy online
- Learning a child rights perspective on children's privacy
- Learning chances of participating children to discover their own understanding of privacy and hounor

Discussion Facilitation:

For the entire break-out group discussion there will be a host. The host will introduce the topic and agenda as well as guide through the whole session. Each break-out team will be joined by one expert as well as one team organizer. To encourage a lively but still structured discussion, each round will start with a question or hypotheses priorly prepared by us. A template will help the discussion-groups to document their main aspects and outcomes. The organizers will collected the outcome-templates and display them for the presentation. For the closing discussion we will provide a structure and one of the speakers will moderate this part.

Online Participation:

We will inform people from our diverse network about the date and topic and policy questions of our workshop, that they are able to participate personally or online to bring in their perspective and questions. Our network includes persons from all different stakeholder groups in different countries, governmental, technical community, private sector, civil society, youth experts.

Proposed Additional Tools: Twitter/ Instagram: One of the organizers will moderate theses channels during the session.
Realtime Board: Remote participants are invited to join our realtime board. There they can find the questions or hypotheses for each discussion round as well as the outcome template. They are invited to fill out the outcome template and display it on our real time board. During the presentation the particpants can not only review their outcomes but as well see the outcomes of the remote participants at our realtime board.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption
GOAL 17: Partnerships for the Goals

IGF 2019 WS #177 Tackling illegal content online: safeguarding digital rights

Theme:
Security, Safety, Stability and Resilience

Subtheme(s): FoE online
Hate Speech
Human Rights

Organizer 1: Intergovernmental Organization, Intergovernmental Organization
Organizer 2: Intergovernmental Organization, Intergovernmental Organization
Organizer 3: Intergovernmental Organization, Intergovernmental Organization
Organizer 4: Intergovernmental Organization, Intergovernmental Organization
Organizer 5: Intergovernmental Organization, Intergovernmental Organization

Speaker 1: Wolfgang Schulz, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Louisa Klingvall, Intergovernmental Organization, Intergovernmental Organization
Speaker 3: Rio Victoire, Civil Society, Asia-Pacific Group
Speaker 4: Saloua Ghazouani Oueslati, Civil Society, African Group
Speaker 5: Tristan Harris, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

What sustainable solutions to address illegal content online are proportionate, comprehensive and bring accountability to all the responsible parties? How can respect for the human rights that are at stake be incorporated in such solutions? How can regulatory solutions, such as removing illegal online content, and extra-legal measures be balanced and better complement each other? How can the wide range of stakeholders better work together to address this? Who is responsible for determining what content should be removed? How do we balance the need to remove illegal content with protecting freedom of expression? How can regulation to protect human rights be effective in the global online environment? How should we define the role of automated means in tackling societal phenomena online, such as hate speech?

Relevance to Theme: Combating illegal online content, including illegal online hate speech, and minimising its criminal potential and negative impact is a task fraught with difficulties. In addition to raising profound human rights concerns, it also raises questions of how to establish effective instruments in a global online environment that crosses jurisdictions and how, practically, to deal with huge quantity and low quality of content constantly uploaded to the internet. Recognising that we are duty bound to take up the task of identifying and addressing harmful content requires collaboration between a wide range of multidisciplinary stakeholders.
This session addresses both elements, by highlighting the human rights issues at stake and bringing together different actors to discuss how they can work together and develop new tools to respond to the threats posed by harmful content online.

Relevance to Internet Governance: The challenge of addressing illegal online content, including illegal online hate speech, showcases the multi-stakeholder nature of internet governance. Determining what constitutes illegal online content is the responsibility of governments, in line with their human rights obligations, and subject to scrutiny and enforcement by the justice system. However, the global nature of the internet and content platforms, combined with the volume of potentially illegal material on the internet, means that internet companies are essential actors. Transforming established human rights norms and principles into actionable rules to protect rights online is emerging as a core challenge for internet governance.

Format:
Round Table - U-shape - 90 Min

Description: Harmful content pervades the internet. From terrorist content to racist, antisemitic, Islamophobic, homophobic or sexist hate speech, it is a phenomenon that knows no boundaries. Whether driving radicalisation or prompting long-term psychological harm among victims of online hate, its consequences can be devastating, striking at the core of human dignity. Indeed, illegal online content impacts a wide range of human rights, from privacy, data protection and freedom of expression, to effective remedy, non-discrimination and victims' rights.

Combatting illegal online content demands a concerted and comprehensive rights-based approach. Through an interactive, multi-stakeholder discussion focused on illegal hate speech, this session aims to identify some of the key elements of a framework to effectively and efficiently identify and remove illegal content and ensure that human rights are protected online. It will offer an opportunity to reflect on the role of different actors, approaches to regulatory solutions, and the place of on- and offline actions to tackle illegal content online.
The roundtable will consist of brief opening interventions by the subject matter experts (approx. 30 mins) to highlight the instruments they have developed and are working with to ensure take down of illegal online content, followed by a discussion with and between other participants:
Moderator: introduces the subject matter experts, explains the discussion topic and highlights the key human rights issues at stake.
Wolfgang Shultz, Council of Europe: setting out the key components of a clear, rule of law based framework for detecting illegal content, including the role of internet intermediaries and obligations of states in this regard. A special focus will be given to the CoE Recommendation on the roles and responsibilities of internet intermediaries.
Louisa Klingvall, European Commission: highlighting the role of voluntary codes of conduct and how different stakeholders (regional organisations, business, civil society) can work together.
Tristan Harris, Center for Humane Technology: The role of IT companies in identifying and removing illegal content and the practical implementation of content moderation tools applied by them.
Saloua Ghazouani Oueslati, Article 19 Tunisia and the MENA Region: Defining main pitfalls of current regulatory approaches to online content, especially in the context of online hate speech.
Victoire Rio, Myanmar Innovation Lab: Discussing the specific situation in Myanmar and Facebook's responses to violence-inciting messages spreading across the platform in this particular national context.
To support practical outcomes and substantive policy discussions, subject matter experts will be provided with a set of guiding questions prepared by the organisers. These will ensure that each of the key policy questions are addressed. Discussion during the session will be facilitated by keeping the opening interventions short, leaving the bulk of the session for exchanges of questions and ideas with and between the walk-in participants and speakers. Speakers will be encouraged to respond to each other's interventions, and those of the audience.

Expected Outcomes: Discussions are underway at the national, regional and international level – as well as among business – about how best to tackle the phenomenon of illegal online content. This session will contribute to ensuring human rights considerations are hardwired into policy debates by identifying some of the key elements that any regulatory regime needs to take into account. Participants will gain insight into existing instruments to address illegal online content, such illegal hate speech, and learn about the roles that different actors in the process can play.

Discussion Facilitation:

At the outset of the session, the moderator will introduce some key questions to the audience, encouraging them to reflect on them during the opening interventions by the subject matter experts and to contribute their ideas and suggestions on these issues during the discussions. Throughout the session, the moderator will proactively reach out to walk-in participants, encouraging them to not only ask questions, but to share their own ideas and experiences. Speakers will be clearly briefed on the format, and encouraged to ask their own questions to each other and other participants.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: The co-organisers will actively promote the session on social media, encouraging remote participation and exchanges on the issues raised during the discussion. Remote participants will be able to pose questions to subject matter experts and other participants during the session. A special hashtag will be created, digital promotional materials will be published on official online platforms of both co-organisers and finally, both co-organisers will be running social media campaigns with a specific focus on Twitter and Facebook platforms.

SDGs:

GOAL 5: Gender Equality
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption

Reference Document

IGF 2019 WS #185 Reporting on ICT companies' human rights harms: A toolkit

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
FoE online
Human Rights
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: ,

Speaker 1: Afef Abrougui, Civil Society, African Group
Speaker 2: Lena Nitsche, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Alimardani Mahsa, Civil Society, Asia-Pacific Group

Policy Question(s):

Private sector responsibilities and accountability: what are the responsibilities of the private sector in ensuring respect and protection of users' human rights online? How can media and civil society groups use documentation to help hold to account technology and telecommunications companies for their responsibilities and human rights commitments?

Relevance to Theme: When technology and telecommunications companies fail to put in place human rights-respecting commitments and policies, their practices may directly or indirectly result in the violation of users' freedom of expression and privacy rights. Documenting these violations and highlighting the impact of company policies and practices is crucial in holding companies to account and making the case for why they must institute policies that foster and reinforce respect for internet users' rights.
To contribute to ongoing efforts and projects aimed at documenting harms involving internet and telecommunications companies, Global Voices Advox and Ranking Digital Rights partnered together to produce a toolkit to help digital rights groups and advocates effectively report on harms involving internet and telecommunications companies in a way that helps all stakeholders better understand the scale and impact of such abuses.

Global Voices Advox is a project dedicated to protecting freedom of expression and free to access to information online. Ranking Digital Rights works to promote freedom of expression and privacy on the internet by creating global standards and incentives for companies to respect and protect users' rights.

During the session, we will introduce the toolkit and train participants in basic skills of gathering evidence and reporting on ICT companies' human rights harms.

Relevance to Internet Governance: Through this toolkit, we are aiming to help different stakeholder groups better understand the scale and impact of human rights harms involving the private sector. Documentation

is not only useful for civil society groups to hold the private sector accountable, but it can also help companies and policymakers better understand where company policies and practices are falling short in order to put in place more effective policies and mechanisms for a secure, open and free internet, where user rights are respected and protected.

Format:

Other - 60 Min
Format description: We would like to organise a tutorial session of 60 minutes (classroom) since we want to give participants the opportunity to work in groups and use the toolkit. We can still present the toolkit in a Tutorial session of 30 minutes but the session would be less interactive.

Description: We will start by briefly introducing the toolkit. We will then divide participants into different groups, and each group will be assigned a case scenario of a human rights harm involving an ICT company. Using the toolkit, each group will have to develop a plan, outlining the different steps they would follow to report on the case that has been assigned to them. During this exercise, the moderator and the speakers will supervise the groups to address any questions. Each group will then get to briefly present their plan. This will be followed by a Q&A, where the moderator and the speakers get to share tips or answer any other questions on how to effectively report on ICT companies' human rights harms.

Expected Outcomes: - Participants will improve their knowledge on how to effectively document and report on ICT companies' human rights harms.
- Organizers will use participants' questions and feedback to assess the digital rights community's needs and concerns in relation to documentation, in order to build on this toolkit in the future.

Discussion Facilitation:

The moderator will use up to 10 minutes to present the toolkit. Participants will then get to work together in groups. The speakers will oversee group work to make sure that participants understand what is expected from them, and answer any questions they may have. They will then get to present their reporting plans. Twenty minutes will be dedicated for a Q&A so that participants get to ask questions about the toolkit and documentation in general.

Online Participation:

We propose to stream the part where we present the toolkit and the Q&A. Before the session takes place, we will promote the it online and share a link to the toolkit. We will encourage those interested to post their questions about the toolkit and how to effectively report on ICT companies' human rights harms, and make sure that speakers answer some of them during the Q&A.

Proposed Additional Tools: we will use the official IGF conference hashtag to promote the session and encourage people to ask their questions. After the session, we will also publish a blog post on rankingdigitalrights.org, summarising what we did during the session.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #195 IT security in the global supply chain

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):

Capacity Building
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Private Sector, Intergovernmental Organization
Organizer 2: Private Sector, Eastern European Group

Speaker 1: Eva Schulz-Kamm , Private Sector, Western European and Others Group (WEOG)
Speaker 2: Paula Iwaniuk, Private Sector, Eastern European Group
Speaker 3: Sergio Lomban, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

- How can industry, governments and other stakeholders work together to make sure that the digitalization of the global economy is trustworthy, safe and secure?
- What are the baseline requirements for cybersecurity that all business players along the global supply and value chains should fulfill to make the digital economy secure for future growth?
- What legal regulations are already in place but potentially need to be enforced and what new legal regulations should be created to address upcoming threats?
- What role should different stakeholders play in cybersecurity capacity building approaches?

Relevance to Theme: The workshop directly addresses one of the main themes of IGF 2019: Security, Safety, Stability, Resilience. It aims to bring IGF participants closer to identifying the need of collaboration for a more secure digital world.

(A) Relevance of Charter of Trust

Charter of Trust is a joint initiative of the Munich Security Conference and 15 multinational companies (AES, Airbus, Allianz, ATOS, CISCO, Daimler, Dell, Deutsche Telekom, IBM, Mitsubishi Heavy Industries, NXP, SGS, Siemens, Total, TÜV Süd) that operate across various business sectors and are committed to improving cybersecurity in the global economy.
These companies are united in the firm believe that cybersecurity is a necessary condition for the success of the digital economy. Digitalization and cybersecurity must evolve hand in hand; users need to trust that their digital technologies are safe and secure.
To achieve this objective, Charter of Trust has set out 10 principles for cybersecurity. The Munich Security Conference and member companies engage with business partners, regulators, think tanks and academia to define these principles and work on a swift implementation in daily business operations.
Therefore, we believe Charter of Trust can contribute to an aspirational yet pragmatic debate about cybersecurity at the IGF.

(B) Relevance of workshop topic

Cybersecurity is only as strong as the weakest link in a given system. Therefore, the Charter of Trust Principle 2 sets out the aspiration to ensure that global supply chains meet cybersecurity standards. Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards. In the workshop we will discuss questions, such as
- Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
- Encryption: Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
- Continuous protection: Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

The workshop will cover the responsibility of companies and address the need of collaboration on a global scale with further industry partners, governments and as well with civil society. It will also be based on concrete examples of companies from Charter of Trust, and how they overcome security and safety crises.

Relevance to Internet Governance: The digital world is changing everything. Today, billions of devices are connected through the Internet of Things. While this creates great opportunities, it also harbours great risks – ranging from data breaches to serious risks to life and limb where the digitalisation creates complex cyber-physical systems.
To make the digital world more secure, the member organisations of Charter of Trust have joined their forces. Taking the spirit of the Paris Peace Call, which Charter of Trust offically supports, the workshop would focus on how cyber and IT security can be enhanced globally.

Format:
Break-out Group Discussions - Flexible Seating - 90 Min

Description: (A) The issue:
Due to the architecture of the internet infrastructure, national or regional regulatory solutions are of a limited effect, so global cooperation is needed. The Charter of Trust is the beginning of a unique initiative by leading global companies, taking their responsibility on Trust and Cybersecurity.
IT and cybersecurity are topics of intense discussion on a global scale. At the same time, dialogue often raises questions about the options for action of state actors. The complexity of the development of the Budapest Convention shows how challenging global developments are. The Paris Peace Call, in turn, shows the political intent for greater security.

(B) Discussions:
The session should deal primarily with entrepreneurial responsibility in reinforcing cybersecurity standards. The topic will also be expanded to how this cannot be done without the support of governments and public bodies to enforce minimum requirements along supply chains, for example. In the session, we aim to shed light on the complexity of global discussions and define common action corridors e.g.in the context of standardization, certification and possibly regulatory frameworks. The EU framework (Cyber act) could be used as an example.

(C) Agenda:
Although discussion and participants contributions will ultimately drive the agenda, the following will be used to guide conversation:

- The session will start with the introduction of invited speakers and a short ice-breaker presentation by the moderator, to set the scene and map out the journey the conversation will take (10 minutes)
- Speakers will then take the floor in turn to present the above-mentioned topics, each followed by input from the audience (60 minutes).
- At the end of the session the moderator, with the help of the rapporteur will summarize the discussion and ask the speakers and audience to comment on the session's key takeaways (20 mins).

Expected Outcomes: The workshop will bring together leaders from global business organisations as well as regulators and think tanks / academia. It will discuss how the various stakeholder groups could collaborate to enhance cybersecurity alongside the supply chain based on global baseline requirements. The workshop would explore how the private and public sector can work together towards a global framework (of commitments) for cybersecurity.

Discussion Facilitation:

The list below provides examples of the way discussion will be facilitated amongst speakers, audience members, and online participants and ensure the session format is used to its optimum:
Seating: Participants will sit in a circle or semi-circle (room permitting), with seats in the middle for the speakers. An empty chair will be placed next to the speakers. Audience members will be invited to occupy the empty seat at selected times of the discussion, to provide further or new perspectives or challenge the

speakers. This will facilitate discussion by creating an enabling and comfortable atmosphere where all speakers and participants are given an equal footing in the discussion. The moderator will have a prominent seating position and may walk around the room to engage participants.
Preparation: Several preparation calls will be organised for all speakers, moderators and co-organisers in advance of the workshop so that everyone has a chance to meet, share views and prepare for the session. Given the varied background of discussants and audience members, organisers will advertise the session and introduce questions to animate discussion on social media in the run up to the workshop. This will introduce the subject, encourage conversation and create links to other dialogues on the topic taking place in other forums to create awareness and help prepare in-person and remote participants for the workshop. The moderator will have questions prepared in advance to encourage interaction among invited experts and between participants, if conversation were to stall. Potential Q&A's will also be prepared in advance to that every speaker is prepared to respond to any comment
Moderator: The moderator will be an expert and well-informed on the topic and experienced in animating multi-stakeholder discussions. Charter of Trust Secretariat has a long-standing experience of organising events with moderators and panellists. It will suggest a list of potential moderators well in advance and help brief him/her before the event.
During the discussion, questions will be incorporated to encourage responses from participants and everyone will be given equal weight and equal opportunity to intervene. Walk-in participants will be encouraged to participate in the discussion by the moderator who will seek contributions from participants in person and remotely.
The remote moderator will play an important role in sharing the ideas of remote speakers/participants and will encourage their interventions through video.
Reporting: Following the discussion, participants will be encouraged to share their key takeaways from the session through online tools and social media. This will help ensure diverse perspectives raised during the discussion are included in the reporting.

Online Participation:

Ahead of the session, the remote moderator will be involved throughout the workshop planning and organization process to advise on where remote participation will need to be facilitated.
During the session, the online platform will be used to animate the discussion and ensure participants in the room and online will have an equal opportunity to engage. The online moderator will occupy the empty seat on behalf of online participants at any given time they wish to join the conversation.
The moderator will frequently communicate with the online moderator throughout the session to ensure remote participants' views/questions are reflected.
The moderator and speakers will be encouraged to follow the online participation tool throughout the workshop themselves, so that issues brought forward by participants in the chat can be carried throughout discussion. Participants in the room will also be encouraged to use their mobile devices to connect and interact with remote participants.
Social media will also be used to generate wider discussion and create momentum for online participation as the workshop is unfolding. Charter of Trust has wide experience in using social media during events and coordinating between member companies.
Co-organizers will ensure that the workshop is promoted in advance to the wider community to give remote participants the opportunity to prepare questions and interventions in advance and to generate interest in the workshop.
Organizers will also explore the possibility of connecting with remote hubs around the globe and organize remote interventions from participants.

Proposed Additional Tools: Organizers will explore the use of audio-visual material (i.e. videos, PowerPoint slides, images, infographics) throughout the workshop to animate the session and aid those whose native language may not be English.

SDGs:

GOAL 4: Quality Education
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 17: Partnerships for the Goals

IGF 2019 WS #202 Designing an environment of security for a trust & safe ICT

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Security Best Practice
Internet Protocols
Trust and Accountability

Organizer 1: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 2: Technical Community, Latin American and Caribbean Group (GRULAC)

Speaker 1: Angela Mckay, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Kulesza Joanna, Civil Society, Eastern European Group
Speaker 3: Víctor Rodríguez, Government, Latin American and Caribbean Group (GRULAC)
Speaker 4: Bruce Schneier, Civil Society, Western European and Others Group (WEOG)
Speaker 5: Diane Rinaldo, Government, Western European and Others Group (WEOG)
Speaker 6: Bronwyn Mercer, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

How can certification schemes for secure ICT products manage risk of vulnerabilities in ICT technologies such as IoT and, current and future (5G) mobile networks infrastructure in order to foster the thrive of an innovative and cybersecure industry?

Relevance to Theme: The advent of Internet of Things (IoT) and Artificial Intelligence increases the potential social and economic impact of digital security failures. While cybersecurity is transversal and comprises many facets, the workshop will focus on strengthening security of ICT products through certification schemes.
Cybersecurity comprises at least the following aspects: economic, social, technical, law enforcement and national and international security. According to the report of the World Economic Forum (WEF) “The Global Risks Report 2019”, machine learning or artificial intelligence (AI) is becoming more sophisticated and prevalent, with growing potential to amplify existing risks or create new ones, increasing the potential social and economic impact of digital security failures, particularly as the Internet of Things (IoT) connects billions of devices. For example, a number of applications for block chain technologies rely on the use of trusted IoT devices to gather data with the needed integrity. Thus, in order to obtain the benefits of these new technologies, it is necessary to reduce the risk of vulnerabilities in IoT products.
Certification schemes impact on the digital security of the end-users; providing more protection in the cyber space will reduce the negative consequences in other sectors of the society. The sharing of experiences, projects and good practices during the workshop may result in the identification of schemes with similar requirements and approaches that could facilitate the design of applicable digital policies to provide cybersecurity in the entire sector. This workshop will also touch on trade liberalization of digital services since it will help to identify technical barriers of security aspects and to promote the investment on security in the ICT products and services, making them more trustworthy.
Moreover, the workshop seeks to build capacities by exploring technical aspects of cybersecurity, specifically focusing on requirements of certification schemes for secure ICT products such as IoT and incoming 5G mobile networks infrastructure. In this context, it is also important to identify incentives for

industry to continue offering digital products and services that meet these standards.
The sharing of experiences, projects or programs between the different stakeholders can contribute to the creation of an environment that promotes international cooperation on this issues, and to gather evidence on whether this approach to cybersecurity is the most appropiate.

Relevance to Internet Governance: Nowadays it is important to design policies that guarantee a safe navigation environment. The new technology advances increase the potential social and economic impact, both positive and negative. This is why cybersecurity ought to focus on user's protection, data protection, and policy makers and other stakeholders must take it into account when designing policies.
One way or another all the digital activities are interrelated; cross border data sharing increases everyone's risk of being a victim of a cyber-attack; it is everyon's responsibility to diligently implement digital policies. This issue has to be addressed from a multi stakeholder perspective because only the different points of view will effectively help to build a more security digital environment and the appropriate policies.

Format:
Round Table - U-shape - 90 Min

Description: The workshop have the following aims:
• To share and discuss experiences, projects and best practices for secure ICT products through certification schemes in order to identify opportunities and challenges.
• To identify approaches in technical regulations and conformity assessment procedures which may be replicated and, result in standards harmonisation.
• To hold a workshop in order to support capacity building.
• To produce recommendations for further collaboration in the strengthening of cybersecurity.

Expected Outcomes: With this workshop, it is expect to identify and share best practices regarding certification schemes for cybersecure ICT products, building the capacity of stakeholders to face these challenges.
In addition, it is expected to outcome the following:
• Develop and support ICT innovation;
• Promote a secure, resilient and trusted ICT environment;
• Enhance the digital economy and the Internet Economy; and
• Strengthen cooperation.

Discussion Facilitation:

The roundtable will consist about to share projects and best practices for secure ICT products through certification schemes in order to identify opportunities and challenges, to identify approaches in technical regulations and conformity assessment procedures which may be replicated and result in standards harmonization. At the end of each the presentation of each topic, the forum will be open for a session of questions.
In terms of format, the round table will be organized as a facilitated dialogue. Led by the moderator, a diverse range of experts from different stakeholder groups - academia, government, industry, civil society and youth participation – will discuss key questions and issues.
Following the round of questions, experts are invited to give open comments, after which the moderator will turn to those attending the session and invite the audience to engage in the conversation. The proposal agenda is the following: - Welcome and opening comments by onsite moderator (10 min) - Two round of questions (5 min max.) to speaker (25 min each round) - Moderated Q&A with the audience and online participants (20 min) - Closing remarks by onsite moderator (10 min).

Online Participation:

.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #208 Co-regulation against online hate? The EU Code of Conduct

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
FoE online
Hate Speech

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Louisa Klingvall, Intergovernmental Organization, Intergovernmental Organization
Speaker 2: Michela Palladino, Private Sector, Western European and Others Group (WEOG)
Speaker 3: Clara Sommier, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Philippe Schmidt, Civil Society, Western European and Others Group (WEOG)
Speaker 5: Steffen Eisentraut, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

For being a multistakeholder panel, some policy questions will logically be more relevant for actors from a given sector than from another one.

Agenda-setting: To what extent does a voluntary commitment such as the Code of Conduct allow to raise the weight and relevance of a particular item (in this case, hate speech) within a given company's list of priorities, not only at the level of their European headquarters but also more globally? Does the Code of Conduct have a significant positive impact on a CSO's ability to perform their advocacy role on the issue of hate speech?

Norms implementation: What is the added value of the monitoring exercise in terms of effectiveness for the implementation of what can be considered as a soft law?

Norms articulation: From a practical perspective, what is the impact of the recent trend, observed in several EU member states, of introducing hard laws on hate speech?

Safety from hate speech: Considering hate speech as an online harm, how can it be addressed to improve user safety on social media platforms? How can the notion of 'hate speech' be operationalized so as to: a) be satisfactory to all involved stakeholders; and b) allow for implementation across different national jurisdictions at a regional level? Could the way it was operationalized within the EU through the Code of Conduct be extended at a wider scale?

Outputs: Does the main benefit from the Code of Conduct stem from the transparency it brings through the implementation reports, or from the cooperation it fosters among stakeholders throughout the monitoring process?

Relevance to Theme: Hate speech is increasingly considered a priority by key stakeholders in Internet Governance, not least because of its suspected links to extremism and real-life violence. On social media platforms, it inhibits the development of conversations by creating a hostile online environment, thereby

obstructing the very aim of those platforms as they were thought out. As such, this session contributes to the "safety" component of the IGF2019 theme "Security, Safety, Stability & Resilience" through a discussion of the case of a voluntary, multistakeholder framework against online hate speech. Indeed, the EU Code of Conduct against illegal hate speech online represents a cutting-edge example of cross-sector cooperation for the provision of a safe user experience online. Through this panel which brings together many of the actors involved in the CoC and their different perspectives, the aims, results and future prospects of this co-regulatory framework will be explored.

Relevance to Internet Governance: Our proposed workshop is built around the very concept of Internet Governance. As a matter of fact, our topic is nothing but an actual dimension of Internet Governance, since it purports to expose how several stakeholders - public authorities, the industry and civil society organizations - are contributing to the design and the implementation of a specific policy against hate speech by assuming roles that are very different but also complementary to one another. Beyond its content, the format of the workshop is characterized by the very same logic: all the participants in our panel have been chosen in such a way that the voices from all the main categories of actors are heard.

Format:
Panel - Auditorium - 90 Min

Description: MODERATOR (5 min):
- exposes the dynamic of the workshop (including a justification for the intervention order: to reflect the chronological development of the CoC) and the modalities for the participation of the public (Twitter # projected on screen at all times)
- introduces the Code of Conduct and its workings, including the Monitoring Exercise attached to it.
- introduces the first speaker

EU COMMISSION (10-15 min) exposes their perspective on:
- Rationale for the CoC
- Role of the Commission in relation to it
- Role - if any - of EU member states in the process
- Main positive impact and room for improvement

ONLINE MODERATOR (1 min) presents the three selected questions, projected on the screen

EU COMMISSION (5 MINUTES) answers the three questions, under time constraints (timer)

MODERATOR (1 min) introduces next speaker

INDUSTRY 1 (10 min) exposes their perspective on:
- Reasons why their company has voluntarily gotten involved in the CoC
- Characterization of the main challenges faced when moderating hate speech
- Concrete changes introduced to the platform as a consequence of the implementation of the CoC
- Main positive impact(s) of the CoC and room for improvement

MODERATOR (1 min) introduces next speaker

INDUSTRY 2 (10 min) exposes their perspective on:
-Company's stance towards the monitoring exercise
-Specific initiatives to bring stakeholders together (e.g. Dublin meetings)
-Impact of the CoC on the company's awareness of the relevance of hate speech issue and/or the most adequate means to tackle this challenge
-Main positive impact(s) of the CoC and room for improvement

ONLINE MODERATOR (1 min) presents the three selected questions (one for industry 1, another one for industry 2 and a third one for both), to be projected on the screen

INDUSTRY 1 & 2 (2x3 min): each industry representative answers their two questions, under time constraints (timer projected on the screen)

MODERATOR (1 min): Introduces next speaker

CIVIL SOCIETY 1 (10 min) exposes their perspective on:
-The typical role played by the CSO during the monitoring exercise
-Relation to national legislation(s), either existing or under development (e.g.: NetzDG in Germany; legislative proposal against online cyber hatred in France)
-Some initiatives that bring stakeholders together (e.g. Dublin meetings)
-Main positive impact(s) of the CoC and room for improvement

MODERATOR (1 min): Introduces next speaker

CIVIL SOCIETY 2 (10 min) exposes their perspective on:
- The impact the CoC has had on the CSO's relations with other stakeholders
- Their input in the way the monitoring exercise is taking place
- Relation to national legislation(s), either existing or under development (e.g.: NetzDG in Germany; legislative proposal against online cyber hatred in France)
- Main positive impact(s) of the CoC and room for improvement

CIVIL SOCIETY 1 & 2 (2x3 min): each civil society representative answers their 2 questions, under time constraints (timer projected on the screen)

Total time: 83 minutes. No doubt the "extra" 7 minutes would be spent in the process.

Expected Outcomes: From the organizers' standpoint, there is a gap between the seriousness of the hate speech issue and the innovative means put in place by the Code of Conduct to tackle it on the one hand and, on the other hand, the fact this mechanism is still very little known beyond the circle of experts in the area. The presentation of the results of the implementation reports by the European Commissioner Vera Jourova in a formal event allows to raise awareness about it, but it still gets attention mainly from people already interested in the topic. We believe that a workshop on this subject could stand for a (still modest) contribution to communicate about the Code of Conduct.

Therefore, we expect this workshop to gather stakeholders that are used to working together, but this time in a different, outward-looking context, so a new range of actors (such as government officials from departments unrelated to hate speech issues, or civil society organizations with other concerns) become aware of this initiative and get the opportunity to take it as a reference in designing and putting in place their own multistakeholder policy-making process in their own areas related to Internet Governance. Likewise, exposing this innovative (and still recent) mechanism to actors that are not usually involved in it will allow to receive fresh inputs from them.

Discussion Facilitation:

The onsite moderator's introduction will contextualize the EU Code of Conduct against illegal hate speech online, so as to ensure that participants with no prior knowledge of this (co) regulatory instrument are still able to participate.

This panel is designed to be interactive, with the public having the opportunity to engage with each type of actor after they have intervened. Participation will be facilitated by the use of a Twitter hashtag which will allow for the public -both onsite and online- to ask questions about speakers' interventions; and/or to engage with questions from other users posted to the social network (through 'likes'). The online moderator will monitor the hashtag during the session and select questions based on their popularity. Such a device will also allow for the conversation to continue beyond the session should the participants desire so.

Online Participation:

Usage of IGF Tool

Proposed Additional Tools: As exposed above, our intention was to use Twitter but we are ready to rather use the built-in Official Online Participation Platform.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #209 Internet Safety:Data Sovereignty to Cyberspace Sovereignty

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Internet ethics
Internet Resources

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Mikhail Anisimov, Technical Community, Eastern European Group
Speaker 2: Xiaodong ZUO, Technical Community, Asia-Pacific Group
Speaker 3: Yi Shen, Civil Society, Asia-Pacific Group

Policy Question(s):

What roles does government plan in Internet safety?
How cyberspace sovereignty can helps to maintain the Internet security?
What is the relationship between data sovereignty and cyberspace sovereignty?

Relevance to Theme: While talking about Internet safety, it is mentioned more from the aspects of technics, physical and hardware. However, with the deepening understand of Internet, some conceptions at ideological level emerge, such as data sovereignty and cyberspace sovereignty, which were put forward on the basis of Internet safety. Once a conceptual consensus is reached in the future, many network attacks may be prevented or solved under the governments' efforts. Since the conceptions are new and extensive, there exists space for further discussion.

Relevance to Internet Governance: Although Internet governance is conducted in different ways in different countries, some basic principles are still needed to solve international dispute, especially when it comes to Internet safety. This workshop is designed to discuss the "sovereignty" in cyberspace, aiming at exploring how to maintain the network security in different countries with different conditions. It is wished to make contribution to the formation of international rules.

Format:
Round Table - U-shape - 60 Min

Description: 1.【5 mins】Welcome and introduction
2.【10 mins】Presentation about the latest practice of Network safety and data sovereignty.
3.【25 mins】Panel discussion:
Key questions:
What roles does government plan in Internet safety?

□How cyberspace sovereignty can helps to maintain the Internet security?
□What is the relationship between data sovereignty and cyberspace sovereignty?
4.【10 mins】Onsite and online Q&A
5.【10 mins】Summary and Closing.

Expected Outcomes: 1.An consensus on what government should do
2.To show different opinions towards data/cyberspace sovereignty

Discussion Facilitation:

1.The conception of data sovereignty and cyberspace sovereignty are new and extensive, with no consensus being reached yet, which leaves space for further discussion on their definitions and appropriateness.
2.Some experts will be invited to share their opinions, experienced moderator will drive up the atmosphere.
3.Onsite and online participation are both welcomed.

Online Participation:

The remote moderator will have a key role as facilitator to the online participants. During the group activity, remote participants will also be given a question to answer related to the overarching IG question under discussion.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #214 Global Collaboration for Internet of Things Security

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Technical Community, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Frederic Donck, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Taylor Bentley, Government, Western European and Others Group (WEOG)
Speaker 3: Maarten Botterman, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

What opportunities and threats do Internet of Things devices pose to the Internet and its users?

How can government representatives work with all stakeholder groups to increase Internet of Things security and network resiliency?

How can government representatives and global organizations work across borders to create a sustainable, secure IoT market?

How can device manufacturers instill security by design principles in their work? How can they collaborate with other stakeholder groups to enhance IoT security?

Do we need one global standard or set of norms for IoT security? If yes, how should it be developed?

What needs to be done in the next year, five years, and ten years to truly secure the IoT?

Relevance to Theme: The Internet of Things (IoT) security addresses all aspects of the theme, "Security, Safety, Stability and Resilience". Internet connected devices pose serious security challenges to the rest of the Internet, especially considering the scale, vulnerability, and longevity of devices. Compromised IoT devices can be used to form "botnets"; networks of Internet-connected, externally controlled devices.

Botnets can be mobilized to perform large-scale attacks. In 2016, a botnet, known as the "MIRAI Botnet", made up principally of poorly secured Internet connected security cameras performed a distributed denial of service (DDoS) attack on the Dyn, a major Domain Name Service provider for the Internet. The attack not only broke records as one of the largest DDoS attacks, but also made major websites, including Twitter, Amazon, and Netflix, temporarily inaccessible for Internet users in some parts of the world. As more poorly secured devices connect to the Internet, the impact of the next attack could be even larger, destabilizing increasing large and impactful services and sites online.

These security threats are particularly daunting as the number of IoT devices for health-related purposes enter the market each year. Life-saving health devices, such as pace makers and glucose monitors, that are connected to the Internet can pose massive security risks to the individuals that use them – both through the control of the device and the sensitive data it collects.

This creates a pressing need for greater security and safety mechanisms to be built into the devices, and resilience to be built into the networks, servers, and software that transmit and store data from IoT devices in order to reduce the risk of weaponization – for both users and the Internet's benefit.

Relevance to Internet Governance: All across the world, governments, civil society, academics, technologists, and private sector representatives are working together to enhance IoT security. They are forming and carrying out successful multistakeholder processes at a national level, and collaborating on best practices and recommendations on a regional and global level. There are several examples of this collaboration and norm-setting, which will be discussed in detail during the session:
Canadian Multistakeholder Process: Enhancing IoT Security (http://iotsecurity2018.ca)
Le Groupe de Travail pour un Internet des Objets de Confiance (France, https://www.isoc.fr/services/groupe-iot/)
Senegal Multistakeholder Process on Enhancing IoT Security (https://www.iotsecurity.sn/)
Global IoT Security Policy Platform (link forthcoming)

Format:
Panel - Auditorium - 90 Min

Description: This session will bring together government representatives, global organizations, and technical experts to discuss the state of the Internet of Things (IoT), and the importance of collaboration to ensure devices are secured and network resiliency is enhanced. There are currently several multistakeholder processes to enhance IoT security being carried out around the world in order to create and implement best practices and recommendations.

A representative from Canada, which will be in the implementation stage of its process, will discuss why the government partnered with the Internet Society and others to lead this initiative, the best practices and recommendations the multistakeholder group created, and what is being done to implement those recommendations.

A representative from Uruguay, which will be in the beginning stages of its own multistakeholder process, will discuss why they decided to carry out this process, what key outcomes they are working towards, and how they are including global perspectives in the work.

Other panel participants will discuss their own frameworks for IoT security, how they differ or are similar to those developed through the multistakeholder process, and how they are working together to harmonize their differences, including through the Global IoT Security Policy Platform.

This Platform has brought together representatives from government agencies across the globe (including in North and South America, Europe, and Africa) to address the challenges to the Internet ecosystem both by the rising threat of IoT security breaches and network resiliency risks, but also by the multitude of frameworks being promulgated across the globe.

This session will serve as an opportunity for those involved in multistakeholder processes and global collaboration initiatives around the world to discuss their work and the things they have learned from each other. It will also provide an opportunity for participants to ask questions about the processes and learn about opportunities to engage, including by creating their own multistakeholder processes at home with support from the Global IoT Security Policy Platform.

Expected Outcomes: As a result of this session, participants will be able to participate in global, high-level discussions regarding IoT security. It will provide a platform to highlight the work done to date by a variety of stakeholders, solicit feedback on that work, identify new potential partners, and identify future opportunities for collaboration.

Discussion Facilitation:

Moderator will actively engage session participants by reserving at least a third of the designated time slot for questions and conversation. Moderator will also announce at the beginning of the session that questions, comments, and feedback are encouraged throughout. The Online Moderator will actively manage comments and questions through the livestream and on Twitter and will read aloud any relevant questions from the online community.

Additionally, by the time of the session, all panelists will have met in person at least once before and will be familiar with each other. This will allow the session to function more as a conversation, as opposed to rote question and answer.

Online Participation:

Online moderator will actively track the online participation tool for questions and comments and will voice all relevant questions in the room for response.

Proposed Additional Tools: Online moderator will actively monitor Twitter and respond to questions or comments.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 17: Partnerships for the Goals

IGF 2019 WS #217 Mitigating Cyber Harm and Organized Irresponsibility

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)

Speaker 1: Belisario Contreras, Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)
Speaker 2: Eneken Tikk, Civil Society, Eastern European Group
Speaker 3: Nayia Barmpaliou, Civil Society, Western European and Others Group (WEOG)
Speaker 4: Klara Jordan, Private Sector, Eastern European Group

Policy Question(s):

- Inclusive understanding of harm subjects/ stakeholders:
Which groups could potentially be affected by the unavailability of a technology-enabled service/ digitally stored data (or its unauthorised disclosure or manipulation)? How do the experienced effects differ between groups? Are all these types of potential harms equally considered in national risk assessments? Is reporting on these harms sufficiently integrated and linked to their underlying causes to facilitate reliable triaging of risks? Which conceptual, financial, political, or other barriers currently exist that limit the wholesome consideration of harm stakeholders?

- Risk management responsibilities:
Based on which criteria and in which steps do risk management responsibilities need to be extended from individual/ group/ organizational level to relevant national authorities? How can subsidiarity be effectively integrated in the distribution of risk management responsibilities? Which risks require proactive and preventive national management to avert systemic consequences? Which safeguards are needed to avoid that the allocation of risk management responsibilities to national authorities does not abet moral hazard by absolving risk-accepting and -producing actors from accountability? How can responsibilities for preventing harm and for mitigating harm be distributed to ensure that a transfer of responsibility for the mitigation of harm does not result in increased risk acceptance, as responsibility is outsourced?

- Challenges in measuring and comparing cyber harm:
Are all types of harms, caused by cyber incidents, currently sufficiently reflected in existing metrics? To what extent does the absence of established metrics for certain types of harms lead to discounted considerations of these harms in risk assessments? Which additional metrics are needed to avoid that risk assessments reinforce any existing biases in the measurement of harms? How can metrics account for subjective differences in the impact of harm (e.g., small enterprises and large transnational corporations will experience the loss of $10,000 with varying significance)? How can measurements of different types of harm be effectively compared with each other, to facilitate prioritised responses?

Relevance to Theme: Much like economic prosperity and a healthy digital environment depend on online security and safety, safeguarding security and safety requires a network-based understanding of risks that need to be mitigated – how they interrelate and enable each other. Building resilience for the digital ecosystem does not stop at identifying and strengthening the weakest link. The very links themselves require careful exploration to uncover possibilities for harms to cascade and for their effects to latently proliferate to new targets. Risk assessments need to broaden their scope to consider these cascading consequences and additional vulnerable stakeholders – most of whom will otherwise insufficiently prepare for these knock-on effects because of incomplete understandings of risks that are accepted on their behalf and of their own technology dependency.

Relevance to Internet Governance: The pre-emptive management of whole-of-society risks relies on inclusive coordination and communication. Where these efforts are limited to narrowly defined communities or discussed in silos, risks are only partially addressed – in as much as they are relevant to the specific interest of any such group of stakeholders. This selective vision on risk can allow potentially more impactful effects of the same hazard to spread and fester as the group-specific security definitions are unlikely to manage all risk aspects required to protect all of society and to stop harms from cascading to other vulnerable groups.

Drawing on the diversity of the Internet governance community, this panel seeks to deepen the understanding of neglected vulnerable groups that risk assessments need to involve and consider to develop a reliable picture of the risk landscape.

Format: Panel - Auditorium - 90 Min

Description: Growing yet elusive technological dependence has given rise to an increasing displacement of the cause and effects of cyber incidents. Enabling social progress and economic prosperity, the adoption of new interconnected technology has embedded an ever-expanding part of national wellbeing in a shared, literally networked, ecosystem. Social, economic, and political functions have become inherently reliant on this technological backbone. In embracing these (inter-)dependencies, we as societies have created and accepted qualitatively new risks of systemic proportions – not always in full consciousness. Overseeing and managing this vast, riven risk landscape poses unprecedented challenges to societies. To rise to these challenges, as societies we need to rethink how we organise responsibilities for anticipating, detecting, preventing and mitigating risks. These efforts require us to deepen our understanding of how risks, if narrowly managed, can cause harms to cascade and proliferate to vulnerable groups previously neglected in risk assessments. Discussions of this panel seek to explore solutions in support of the early and active detection of technology-enabled risks and an agile response to unanticipated consequences, to protect all sides of national welfare in the digital space.

To strengthen consideration of the full spectrum of potential harms and vulnerable groups, this panel brings together perspectives from civil society on the socio-technological nexus of risks and the importance of addressing risk perceptions as well as actual risks; from government on mounting an inclusive and proactive national risk management response; from the risk management community on strategies and tools for expanding risk awareness and on how to scan for interdependencies; and from the industry on advancing public-private sector cooperation and cost-effective solutions for SMEs.

Expected Outcomes: Sharing and evaluating best practices, the workshop aims to develop insights into:
- mechanisms for the proactive identification of unanticipated or latent harms and risks of cascading consequences as well as neglected vulnerable groups;
- the allocation and transfer of risk management responsibilities to enable the prevention and early mitigation of harms; and
- elements of an inclusive national risk management framework that reduces tensions between private benefits and societal harms.

These insights will further inform the Cyber Harm Framework the Global Cyber Security Capacity Centre is currently developing, which will be openly available to the community. The Framework seeks to advance a more inclusive approach to cyber risk assessments by enhancing the consideration of neglected vulnerable groups and underappreciated types of harm, to enable the earlier detection of risk overall and the design of more cost-efficient preventive responses.

Discussion Facilitation:

Holding this panel at the IGF would provide a unique opportunity to hear from a diverse set of stakeholders. Gathering a wide range of perspectives on the same risk from different angles can offer a more complete picture and highlight the views of groups overlooked in traditional risk assessments. During the session, the moderator will explicitly ask online and onsite participants to take part in the debate and, in close coordination with the online moderator, will ensure that audience contributions and questions are integrated into the discussion as a valuable part.

Online Participation:

In advance, the opportunity for online participation will be promoted on all available channels of the participating organizations, including email, telephone, mailing lists, and social media. The three core parts of the communication will be the importance of online participation for the outcomes of the IGF, the invitation to submit questions in advance, which will be discussed and prioritised in the session, and technical information on how to weigh in via the official online participation platform.

Proposed Additional Tools: This panel will seek to facilitate and actively encourage inclusive participation in the proposed discussions, before and during the session through the strategic use of the official online

participation platform, Facebook Live and Twitter.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 12: Responsible Production and Consumption
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #218 Deliberating Governance Approaches to Disinformation

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
FoE online
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)
Organizer 4: Civil Society, Western European and Others Group (WEOG)
Organizer 5: Civil Society, Western European and Others Group (WEOG)
Organizer 6: Civil Society, Eastern European Group
Organizer 7: Civil Society, Asia-Pacific Group

Speaker 1: Jaclyn Kerr, Government, Western European and Others Group (WEOG)
Speaker 2: Jan Rydzak, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Vidushi Marda, Civil Society, Asia-Pacific Group
Speaker 4: Sabine Frank , Private Sector, Western European and Others Group (WEOG)
Speaker 5: Moses Karanja, Technical Community, African Group

Policy Question(s):

- Evaluation of governance approaches: What are the trade-offs of various recent European policy instruments that address disinformation, especially with regard to preserving the balance between freedom of expression and the quality of discourse necessary to sustain democratic governance?

- Multi-stakeholder contribution: What specific opportunities can focused multi-stakeholder assessment of existing policies open in the process of creating future policy instruments and regulatory models on disinformation?

- Improving collaboration and standard-setting: What role should different stakeholder groups - including private sector Internet platforms, governments, and civil society actors - play in defining the standards for acceptable content in light of the dual need for freedom of expression and protection against the harmful effects of online content? How can globally accepted standards be developed? How can policy developments on the subject in different geographic regions inform each other? What unexplored forms of collaboration would help in fighting disinformation and ‘fake news’?

Relevance to Theme: The session responds to the theme’s focus on defining overarching standards for acceptable content within the substrand of disinformation. It uses a collaborative, multi-stakeholder

framework with a proven record in impacting policy to assess the impact, similarities, and differences among three policy instruments, all launched or proposed in the European Union, but globally relevant. This highlights the diversity of frameworks and categories of instruments (e.g., self-regulation, legislation, advisory reports, public-private partnerships) that have been applied to disinformation, leading to a more detailed and informed international conversation. The approach creates a basis for comparison and further collaborative work on the issue across various domains of expertise, including academia, civil society, the private sector, and other communities.

Relevance to Internet Governance: The session will drive the cross-regional search for additional stakeholders (policymakers, technologists, netizens) who should be included in the debate on disinformation, and help define their roles. We will base the discussion on a research report that analyses the challenges and options in this field. We will capture the discussion at the IGF workshop and use it to improve these briefing materials to serve the concerned stakeholders better. All participating stakeholders, including government actors, will come out of the exercise with a deeper understanding of the possible regulatory, advisory, and self-regulatory instruments that address disinformation, which will inform future regulation in this space. The session's emphasis on cross-regional insight broadens its relevance to Internet governance write large rather than a single geographic region.

Balanced Briefing Materials can contribute meaningfully to deliberations about Internet governance solutions. Balanced Briefing Materials and deliberative methods offers a way to both provide a shared understanding of the challenges and options for Internet governance issues and to measure the impact of individual discussions.

Format:

Round Table - U-shape - 90 Min

Description: This session will use innovations in the deliberative method to assess the strengths, shortcomings, and effects of three policy instruments that address disinformation and content moderation at scale in the European Union. It seeks to compare these approaches using a methodology that relies on objective ground truths and a series of deliberations conducted prior to IGF. Participants will identify cross-regional confluence points with regulatory and other actions that are being undertaken outside Europe, and develop best practices that cut across geographies. Ultimately, the session will help develop informed solutions that maximize the possibility for freedom of expression and democratic discourse while mitigating the harmful consequences of disinformation in online spaces.

The conversation will center on France's Law Against Manipulation of Information (2018), the UK House of Commons Digital, Culture, Media & Sport Committee's 'Online Harms' white paper and proposal (2019), and the EU Code of Practice on Disinformation (2018). These three policy instruments represent distinct regulatory and self-regulatory approaches to content moderation and the proliferation of disinformation online and offline.

In the months leading up to the session, two or three small-group deliberations will take place online, with the use of specially commissioned Balanced Briefing Materials and an automated smart moderator tool designed and tested at Stanford. These exercises will use the deliberative method. The materials, generated in the preparation phase, consider trade-offs between policy options on governing disinformation. These sessions will include IGF participants as well as other Internet governance stakeholders. Before the deliberation, we will survey our sample of stakeholders using questions related to the policy instruments. Those who take part in the deliberation will be re-polled immediately afterwards; their changes of opinion represent the new conclusions the public might reach if they had the opportunity to deliberate through an informed and fact-based process. We expect to demonstrate that debates based on shared ground-truth briefing materials provide a basis for informed decision making in the realm of content governance and freedom of expression online as a whole.

Building on these online deliberations, the session at IGF will be structured as follows.

(1) Introduction and overview of deliberative method (10 min.): The research team will open with an overview of the briefing materials, the rules governing the deliberation, and the performance of the automated moderator tool. Members of the research team will also briefly discuss findings and lessons from the deliberation on NetzDG at IGF Deutschland in 2018, and encourage participants to review the briefing materials for that session separately.

(2) Expert discussion of deliberation results (60 min.): The organizers will present a snapshot of the results of the deliberative polls, focusing on reported changes in participants' positions on different components of each instrument and level of knowledge following the deliberation. Invited experts familiar with the three laws and their links with policies being developed in other regions will assess the deliberations' contributions to outlining best practices for addressing disinformation.

(3) Debrief and Q&A (20 min.): The organizers will summarize the session, announce next steps, provide a brief preliminary assessment of the applicability of the deliberative method to the global discussion on disinformation, and allow space for any additional questions.

The session builds on numerous successful implementations of the deliberative method, including the Deliberative Poll on the European Union (2009), a pilot deliberation on multi-stakeholder collaboration for extending Internet access to the next billion users (IGF 2015), a deliberation on encryption (IGF 2016), and the recent IGF Deutschland (2018), at which participants debated the German 'NetzDG' law using the same methodology.

Expected Outcomes: The deliberative method is geared toward producing practical outcomes. Past Deliberative Polling exercises provide strong evidence of significant and measurable knowledge gains and changes in opinion among participants. We expect that this will be the case for this workshop as well, as not all participants will be conversant in all three policies at the outset. The workshop will produce the following outputs: (1) polling results measuring changes in levels of knowledge and preferences among participants, (2) a set of Balanced Briefing Materials with multiple uses outside of the deliberative process (e.g., comparative analysis of policy instruments), and (3) a report on the findings.

The workshop will also lay a foundation for further deliberative exercises on the development of the three policies. The results of the workshop will form the basis for advisory opinions on these policy instruments, which will play a direct role in defining best practices for future legislation, particularly in cases where legislative proposals have yet to be formulated.

Finally, in the broadest sense, the workshop will showcase the utility of a novel methodology to carry out an informed discussion and analysis of laws that govern online content. The method helps counter misinformation on existing and proposed policy instruments, guard against cognitive barriers that could marginalize or exclude individuals, and lead to reasoned decision-making. All three instruments discussed were published in 2018-19; this session would be their first comparative multi-stakeholder assessment. This will help distinguish the exercise from sessions that tackle disinformation as a broad issue without explicitly addressing policy instruments as well as from those that analyze a single instrument in isolation.

We are happy to collaborate with other workshop organizers in the same field to ensure that our session is complementary and to drive collaboration in this space beyond the IGF.

Discussion Facilitation:

Interaction is critical to the success of the deliberative process. The IGF session will be actively moderated to ensure feedback not only from European actors, but from stakeholders from other countries who are interested in the cross-national diffusion of policy solutions on disinformation. The pre-IGF small-group deliberations will be guided by moderators well-versed in the method, who will prioritize giving every participant a chance to express themselves. This will drive the changes in levels of consensus and knowledge the project seeks to measure. The pre- and post-event polls are designed to maximize inclusion and useful feedback.

Online Participation:

A number of individuals who will participate in the online deliberation prior to IGF might be absent from the event itself. The online participation tool will enable us to receive their input and collect feedback from those who are neither able to participate in the online deliberation nor in the on-site session. The online moderator will be carefully monitoring the queue so that all participants with remarks are heard. We are also ready to devote a sub-block of the session to comments from the online platform if there are numerous comments.

SDGs:

GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #224 Social Media Content Moderation in Conflict Zones

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Civic Engagement online
Human Rights
Internet ethics

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, African Group

Speaker 1: caroline sinders, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Nadim Nashif, Civil Society, Asia-Pacific Group
Speaker 3: Phyu Phyu Thi, Civil Society, Asia-Pacific Group

Policy Question(s):

Where is the middle ground between security and privacy? Content moderation and suppression of freedom of speech?
What role should Internet platforms play in defining the standards for acceptable content in light of freedom of speech and international law?
How can globally accepted standards for human rights law be reflected in digital policies of social media companies?
What is the impact of social media companies cooperation with governments and regimes in conflict zones and occupation contexts?

Relevance to Theme: For people living in conflict zones and under military occupations, many essential human rights are under threat or violated. Being able to access the internet securely and safely is one of the ways that people can gain some sense of stability and increase their resilience during a conflict or occupation. This panel will enable experts working in conflict zones and living under occupation to share the impact that relationships between governments, social media companies, civil society and the public are having on human rights and digital rights in conflict zones.

Relevance to Internet Governance: During conflict and under occupation, oppressive regimes are increasingly targeting ICT systems and users as strategies for political, economic or social control. Social media companies continue to purport that they are neutral tools that enable freedom of expression and to connect people in a democratic way to the public space. But despite this vision, digital rights advocates know that social media is also being weaponized; limiting freedom of expression, enabling the spread of hate speech, fake news and propaganda that result in real world conflict and enable regimes to violate

human rights. The massive amounts of data that social media companies like Facebook collect (online and offline), make them some of the world's most sophisticated surveillance structures on earth. Over time, journalists, academics, policy makers and activists have proven that social media companies do not sufficiently monitor misinformation and mis-use of information; users data is insufficiently protected, policies do not protect people's rights, lack transparency, and are unfairly enforced in ways that can support regimes that violate human rights.

This panel will provide insight into the impact that current practices and policies, or lack of policies, have on the human rights of people living in conflict zones and under military occupation. It will provide recommendations from civil society members on policies and practices for social media companies and civil society organizations that can provide solutions to problems arising in these contexts that support upholding international law and protecting human rights.

Format:

Panel - Auditorium - 90 Min

Description: The panel seeks to address the purported position of social media companies to support democracy and how their policies and practices in conflict areas -- in particular content moderation policies -- are impacting human rights and social movements. Experts from the occupied Palestinian Territories, Myanmar, Kashmir and Ukraine will share how the policies of social media companies impact the saftey and security of people in conflict and occupation contexts and share insights on how policies of social media companies can be developed to uphold international law.

The 60 minute session will begin with the moderator opening the panel and giving a example of how content moderation policies of social media companies in conflict zones and occupations impacts the digital safety, security and human rights of people (5 minutes). The moderator will then introduce the panel members by giving a quick bio of each panelist and their qualifications (3 minutes). The moderator will then pose a set of questions specific to the panelists that will illustrate 1) how content moderation policies and practices are impacting the rights of people living in conflict zones and under military occupation 2) what strategies they are employing to increase safety and security 3) what social media company policies and practices would improve the safety and security of people living in conflict zones and under military occupations. The moderator will ensure that time constraints are taken into account and that speakers keep on topic and with equal opportunity and time to speak (30 minutes). Each panelist will have the opportunity to give closing remarks and before the question and answer section will be opened. This Q&A section will include interaction with a live audience and and online audience who will be given equal time to participate; in total 4 - 6 questions will be answered (15 minutes). The moderator will close the panel and thank the panelists for their contribution (3 minutes).

The rapporteur will take notes of the discussion and draft a summary report that outlines the main challenges for people in conflict zones and living under occupation to safely access and utilize the internet for political, social and economic engagement. The summary will include recommendations for content moderation policies from the panelists that will be submitted to the IGF Secretariat and shared via the panelists online networks.

Expected Outcomes: R1: Increased understanding of how the relationships between social media companies and regimes impact human rights in conflict zones and for people living under military occupations. R2: Raised awareness of the importance of access to safe Internet for resilience of people living in conflict zones and under military occupations. R3: Exchange of information and best practices among digital rights advocates working in conflict zones and occupation contexts shared. R4: Solutions to the issues arising from the use and misuse of the Internet, of particular concern to everyday users in conflict zones and living under occupation. R5: Content moderation policy recommendations for social media companies, governments and civil society that uphold international law and ensure the safety, security and stability of people residing in conflict zones and living under occupation. R6: Strengthen and enhance the engagement of stakeholders operating in conflict contexts existing and/or future Internet governance mechanisms.

Discussion Facilitation:

In order to facilitate and encourage interaction during the session, as well as multiply the impact of our workshop, we will have specific activities prior, during and after the session. In order to encourage people to participate during the session, the organizers and the panel speakers will share the session with our networks by posting it online and sharing it across social media. This will also include a sign up for people who want to be notified to join the panel online. During the panel the online moderator will open the necessary technical equipment which may include cooperation with Friends of IGF or other streaming of the panel, zoom / facebook live as well as the official online participation tool. Participants will have the chance to ask questions and to participate in an audience poll utilizing a link that we will share at the panel in both online and offline space. In order to facilitate discussion, an online moderator will pay attention to the questions from the remote participation hub and during the question and answer session ensure that their questions are being asked to the panelists. This will also enable us to gain the emails of people attending the session and share the report with them following the session. The report, the livestream and other photos or materials collected from the panel will be shared online via the networks of the organizers, speakers and their partners (including the Association for Progressive Communications). We will document the reach and engagement on the tools and would be happy to share them in a report as well.

Online Participation:

We are unclear at this time how to utilize the online participation tool and were not able to find enough documentation about this online. However, we would like to include engagement utilizing this online tool with further information about its capabilities. At the least, we will be encouraging people to register to the panel using the official online tool.

Proposed Additional Tools: We are planning to utilize a video conferencing software or Facebook live, as well as the official online participation tool to encourage people to directly participate and ask questions and share their reactions of the event. If using facebook, these interactions can be record as well and shared following the event. We would also like to enable people to participate in an online poll at the panel and virtually in order to share information about the perception of audience members and gauge their reaction to the policy recommendations being proposed, and determine some of what they have learned from the panel.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 12: Responsible Production and Consumption
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #240 Tackling Cybercrime in Tertiary Institutions

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Technical Community, African Group
Organizer 2: Government, African Group
Organizer 3: Government, African Group

Speaker 1: Deborah Adeyemo, Government, African Group
Speaker 2: seyi osunade, Technical Community, African Group
Speaker 3: Owen Iyoha, Technical Community, African Group

Policy Question(s):

1. How do tertiary institutions build capacity to combat cyber crime?
2. Is the Nigerian Cyber crime Act of 2015 sufficient as a legal framework?
3. How should data be shared amongst collaborating institutions?
4. Should the establishment of CSIRT/CERT be institutional or collaborative?
5. What skills are required by cyber crime personnel?

Relevance to Theme: Nigerian educational and research institutions are early adopters of digital technology. There has been huge investment in digital infrastructure by institutions, donors and the government. Cyber attacks are being launched from within institutional networks which have embarrassed institutions and led to blocked IP addresses, virus attacks and lost data. Institutions are integrating security framework into their digital ecosystem. How effective are they and what is the best way forward?

Relevance to Internet Governance: This work relates to how the Internet is provided and managed at educational and research institutions within a region in Nigeria. The institutions are expected to have the same principles but the implementation of Internet access and investment into digital infrastructure is different. In this workshop, an acceptable framework for all issues related to cyber attacks in academic institutions will be discussed.

Format:
Birds of a Feather - Auditorium - 30 Min

Description: The workshop will highlight the current cyber crime framework and infrastructure in Nigeria. The implementation in Nigerian educational and research institutions on a regional basis will be discussed. The resources and personnel needed to have a successful cyber security implementation will be listed.

Expected Outcomes: The workshop is expected to provide a roadmap for the implementation of cyber security units at a regional level in Nigeria i.e. Oyo State. Also to identify the skillset needed for cyber security professionals within the educational industry.

Discussion Facilitation:

A social media campaign will be launched locally in Oyo State, Nigeria to ensure remote participation. A remote participation location will be set up at University of Ibadan, Nigeria to facilitate participation for free.

Online Participation:

A remote participation location will be set up at University of Ibadan, Nigeria to facilitate participation for free.

SDGs:

GOAL 4: Quality Education
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

IGF 2019 WS #241 Understanding Hate Speech: research for informed policy

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
FoE online
Hate Speech

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 3: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 4: Civil Society, Latin American and Caribbean Group (GRULAC)

Speaker 1: Natalia Torres, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Susan Benesch, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Guilherme Canela Godoi , Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

How can we develop sound research to understand the variety of phenomena comprised under the term hate speech? Which are the methodological strategies that can be implemented in order to advance in the comprehension of the phenomena? Are there any implication on the studies depending on who is in charge of these research experiences (Government, academia, intermediaries)? How can we inform other actors on our advances? Is possible to think in an articulated strategy of research (multitakeholder, country-based, regionally oriented, global)?

Relevance to Theme: Hate speech has been defined as those expressions that intimidate, oppress or incite hatred or violence against a social person or group based on their race, religion, political choice, gender, among other characteristics. Per UNESCO, the concept ¨may also extend to expressions that feed an environment of prejudice and intolerance in the understanding that such an environment can encourage discrimination, hostility and violent attacks directed at certain people¨. It may generate serious consequences in terms of the social fabric and participation in public space and its impact may hinder the political life of a community. If certain groups are excluded from public debate, it undermines the plurality, openness and diversity demanded for the free exercise of freedom of expression. This phenomenum is aggravated by it happening online: content rapidly becomes viral and may be reinforced by disinformation. Studies on the matter are scarce. According to UNESCO´s report, there are rare experiences on research. UMATI research project, which began in September 2012, ahead of the Kenyan elections of March 2013, implemented a monitoring experience to analyze Kenyan online discourse to estimate both the occurrence and virulence of hate speech. This experience was only possible because of the thorough study on the term of hate speech and the differentiation of phenomena that provided The Dangerous Speech Project. Another experience that worth mention is the one developed by the Italian researchers at the University of Turin. Along with these experiences, the efforts done by intermediaries to identify these expressions circulating in their platforms and some monitoring experiences of governments, such as the one carried by the governmental Observatory on Racism and Xenophobia of Spain. CELE will launch its observatory on hate speech this year, that would be the first experience in Latin America.
As can be seen, research studies on hate speech are rare unicorns in internet related environment. Even when various international bodies have called for the implementation of policies that allow reverting the general ignorance of the magnitude of the circulation of hate speech, the conditions that cause its emergence or the effects they produce. The reports of the European Commission Against Racism and Intolerance (2016), the Special Rapporteurship for Freedom of Expression of the OAS (2015), the Special Rapporteurship on Freedom of Expression of the United Nations (2012) and the Rapporteur Special for

Minorities of the UN (2015) have expressed, coincidentally, the need to develop studies that allow us to advance in the design of preventive policies that collect and analyze data on these phenomena and thus strengthen the decision-making processes, design, elaboration and implementation of public policies to better protect population groups at risk.

Relevance to Internet Governance: The workshop will contribute to orient the generation of monitoring experience on hate speech and the coordination between multiple actors in a multi-stakeholders scenario.

Format:

Debate - Classroom - 90 Min

Description: The workshop will be developed as follow:
- A brief description of each of the experiences. The classroom will have mini posters on the experiences on their walls, in order to invite the public to walk through them.
- Leading by an onsite moderator, policy questions will organize debate, where referents of experiences will summarize learnings and obstacles.
- A online moderator will gather questions from IGF platform and social networks, organize them and present to moderator. This communication specialist will also share key aspects of discussion through social media and organize one in depth interview with specialized press to spread the reach of the discussions.

Other activities:
- Rapporteur will prepare a document resuming policy discussions.

Expected Outcomes: The objective of this session is to contribute in the generation of an epistemic community on the understanding of hate speech. In this sense, the expected outcomes are:
- to build a network of information exchanges and a rich community where researchers, agents and officials can share their questions and achievements on monitoring experiencies.
- to highlight the need of further research on the matter.

Discussion Facilitation:

The onsite moderator will present posters and presenters and organize debate through policy questions, where referents of experiences will summarize learnings and obstacles.

Online Participation:

A online moderator will gather questions from IGF platform and social networks, organize them and present to moderator.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

Background Paper

IGF 2019 WS #247 Internet de-tox: A fail-proof regimen to end online sexism

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

FoE online
Hate Speech
Trust and Accountability

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Intergovernmental Organization, Western European and Others Group (WEOG)

Speaker 1: Mariana Valente, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Nanjira Sambuli, Civil Society, African Group
Speaker 3: Jai Vipra, Civil Society, Asia-Pacific Group

Policy Question(s):

An effective online content governance framework that balances freedom of expression and freedom from misogynistic speech continues to be a policy challenge for gender inclusion. The attacks that women face in the online public sphere reflects social prejudice that is intersectional. For instance, in India and Brazil, caste and race are ever-present in the hate that women encounter online. This reinforces social and gender stratification, amplifying discrimination and contaminating public discourse. Building on empirical research on gender-based hate speech in India and Brazil, this workshop will address the following policy questions:
(a) What are the legal-policy constructs about sexism and misogyny in India and Brazil, respectively, and how adequate are they in tackling gender-based hate speech online?
(b) What new normative benchmarks that address gender-based hate speech are needed to enable women's free expression online without the threat of highly punishing costs of online participation?
(c) What actions should policymakers, internet intermediaries and civil society organisations undertake, for gender-transformative change, including in online cultures?
(c) What good practices on legal-policy frameworks, platform policies, and cultural interventions are instructive, in this regard?

Relevance to Theme: A central concern of the thematic area "Security, Safety, Stability and Resilience" is the creation of a healthy digital environment that enables women to freely exercise their voice, without the shadow of violence perpetually looming over them.

Relevance to Internet Governance: Content regulation has been a long-standing priority area of engagement for the Dynamic Coalition on Gender and Internet Governance and this has acquired a lot of traction in the past couple of years. Feminist activists and groups across the global South have been calling out the increasing sexism and misogyny in dominant online spaces and the inadequacy of existing responses of states and platform intermediaries. The Special Rapporteur on Violence Against Women (part of the Special Procedures Mechanism of the UN OHCHR) has called attention to the need for immediate cooperation of states, platform intermediaries and all other stakeholders in this regard, in order to evolve a robust response to the issue that is rooted in the broader framework of human rights.

Sexism and misogyny have tended to be historically ignored in legal discourse. Democracies have tended to tolerate disparaging remarks about women in the public sphere. However, as women have stormed the Internet, seizing online spaces to speak up, build community and assert their rights, this normalization has become contested. Further, what existing research points to is that in the online public sphere, hate against women is based on their differential locations – tying in with their caste, racial, religious, ethnic and sexual identities.

While social media platforms acknowledge the challenge and are exploring new ways of modifying techno-design and upgrading community standards in context-appropriate ways, efforts need to be based on informed discussions rooted in feminist frameworks. Legal approaches need a new normal. Civil society organizations, especially women's rights activists working on building alternative communicative cultures for the digital society, need to present ideas and concepts that can inform norm development by the state and by social media companies. This workshop will bring initial insights from an inter-country research project exploring legal/institutional/socio-cultural responses to tackle online hate speech against women in Brazil and India, in order to trigger an informed debate and discussion in this emerging policy area.

Format:
Round Table - U-shape - 90 Min

Description: The agenda for this session, organized as a roundtable, is as follows:

(a) Deep dive into context-specific manifestations of online sexism and misogyny and identifying the key legal-institutional and socio-cultural challenges of the issue
(b) Identification of a roadmap for strategic action through exchange of ideas on legal, policy and community action, including:
- overhaul of legal frameworks
- articulation of the roles and responsibilities of platform intermediaries
- efforts to challenge deep cultures of patriarchy that normalize sexism and misogyny in digitally-mediated social interactions

The moderator, Scott Campbell from UN OHCHR, will open the roundtable (2 minutes) by flagging the urgency of evolving a multi-stakeholder roadmap rooted in human rights frameworks for tackling online sexism, misogyny and violence. He will then invite 4 expert inputs of 6-7 minutes (28 minutes) each, to frame the conversation:

Mariana Valente, InternetLab, Brazil and Jai Vipra, IT for Change, India will present reflections about their country contexts, from their ongoing IDRC-supported research collaboration on this issue. The intent of these presentations is to raise provocative questions about the adequacy of global community standards of platform intermediaries and global North approaches to free speech regulation in addressing this issue in democracies of the global South.

The representative from Facebook, South African Development Community region, will reflect on the platform's efforts to improve and refine its community standards, taking into account cultural sensitivities, and enhance responsiveness to complaints about gender-based hate speech and cyber violence. S/he will focus on the challenges in this regard.

Nanjira Sambuli, Web Foundation, Kenya will discuss the major gaps in existing responses to the issues, reflecting on actions of states, platform companies, and civil society organizations, including the gaps in inter-stakeholder cooperation.

This segment of the session will be followed by a round table discussion (50 minutes) where 15 participants will be encouraged to make 2-3 minute long interventions, reflecting on the intersections between their contextual experiences of dealing with online sexism and misogyny and the issues raised through the expert presentations. The intent of this collective brainstorming is to evolve a robust action plan to address the issue, including the evolution of global normative benchmarks. These participants who will be allotted speaking slots will be identified prior to the session by the organizing team -- both through a process of online sign-ons from interested individuals through widely publicizing the workshop in the lead up to the IGF and extending individual invites to experts in this area who are known to be attending the IGF. In the process of allocating the speaking slots, care will be taken to ensure that there is adequate representation of women and girls who are active in public-political life, and individuals from marginalized socio-structural locations (eg. sexual orientation, gender identity, geography, and age).

At the end, each of the 4 speakers will have 2 minutes (10 minutes) to wrap up on what they see as critical elements for a 'de-tox' regimen to end online sexism and misogyny, by building on key elements raised in the plenary discussion.

Expected Outcomes: (a) Trigger a robust, evidence-based discussion about the context-appropriate responses to online sexism and misogyny, especially in the global South
(b) Trace the contours of a multi-stakeholder road map to tackle this issue, focusing on the dimensions of legal-policy reform, roles and responsibilities of platform intermediaries, and cultural change.

Discussion Facilitation:

The format of the session makes for engaged debate and dialogue -- a roundtable that is kickstarted with trigger presentations to catalyse reflective engagement. 40 minutes have been earmarked for plenary discussion to ensure that participants have adequate time for interventions.

Online Participation:

The online moderator will invite comments/reflections on the trigger presentation from remote participants which she will feed into the plenary discussion.

SDGs:

GOAL 5: Gender Equality

IGF 2019 WS #259 Navigating Freedom of Expression Online

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Crime
Fake News
FoE online

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, African Group

Speaker 1: Marchant Eleanor, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Sheetal Kumar, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Padraig Hughes, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

How do we foster an Internet conducive to freedom of expression online, on which journalism in particular is not stifled by internet-specific content restrictions in national law, filtering of online content, or network disruption?

How can free speech and safety and security on the Internet (i.e. combating cyber crime, false news, and hate speech) be balanced in national legislation? How can government and civil society stakeholders improve their collaborations for developing norms and standards that protect all of these principles at a national, regional, and international level?

How can stakeholders, individually and collectively, mitigate filtering of content and Internet shutdowns so as to ensure network stability and resilience - a precursor for the protection of freedom of expression online?

Relevance to Theme: Security and safety on the Internet is an imperative but so too are the rights of individual citizens, bloggers, and media to publish public interest content free from undue restrictions in national law. In numerous jurisdictions, speech rights oftentimes conflict with provisions in laws aimed at combating cyber crime and other Internet-related security and safety concerns. i.e. Cyber crime laws that contain overly broad content provisions vulnerable to overreach and abuse.

Relevance to Internet Governance: Navigating a balance between freedom of expression and security online necessitates the input and involvement of multiple stakeholders with a role in internet governance. It requires the forging of collaboration between civil society and state stakeholders in particular - both at a national and global level to develop and institutionalise standards that protect freedom of expression on the Internet while also guaranteeing the safety and security of its users.

Format:
Round Table - Circle - 60 Min

Description: This round table will discuss instances where the right to freedom of expression online has been threatened by provisions in cyber crime legislation as well as blocked or partially restricted access to the Internet. It will address civil society strategies to address these challenges through advocacy and litigation at national and regional levels as well as developing an understanding of state responses and responsibilities.

In many jurisdictions Cyber crime laws in particular have been passed with overly broad content restrictions on false news and hate speech which can be used to impinge upon the rights of citizens, bloggers, and media to report freely in the public interest.

The proliferation of filtering of online content as well as network disruption and Internet shutdowns poses similar challenges to expression rights on the Internet, often justified by national security arguments posited by state actors.

Drawing upon a diverse range of legal, civil society, academic, and state stakeholders, the contours of balancing freedom of expression and security online will be outlined from each of these perspectives. Interaction between speakers, walk-in, and online participants will be encouraged. This with a view to developing an in-depth understanding of the challenge at hand and how to it can be addressed through litigation at a national level and regional level, as well as by collaboratively developing norms and standards by leveraging regional and international human rights instruments and mechanisms.

The workshop structure structure, subject to revision, will include:
1) Moderator's welcome, introduction to speakers and topic (10 minutes)
2) Opening remarks by each speaker (4 x 5 minutes = 20)
3) Moderated discussion between speakers, online and walk-in participants (25 minutes)
4) Closing remarks by moderator (5 minutes)

Expected Outcomes: (1) The development of an in-depth understanding of the challenge balancing expression and security online from the perspective of state and civil society stakeholders.
(2) Recommendations developed for the development, institutionalisation and use of regional and international standards that address this balance.

Discussion Facilitation:

Speakers will be asked to provide their input as concisely as possible and for it to run no longer than five minutes each, thus allowing the session to maximise time for engagement and interaction between speakers, walk-in, and online participates.

Online Participation:

Online participants will able to submit questions and comments through the online participation tool throughout the round table. This opportunity will be promoted through the Media Legal Defence Initiative's (MLDI) facebook page, twitter account, and the live stream that will be available for this workshops. Comments, questions and other forms of engagement will be solicited and then posed to the room by the online moderator at regular, prearranged intervals.

Proposed Additional Tools: The online participation plan for this workshop integrates the use of the organising organisation's social media accounts and the official participation tool. As stated above, MLDI's significant reach on twitter and facebook will be used to direct off-site participants to the online participation tool through which they will be able to pose questions or make comments.

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #268 Coping in an era of misinformation:Who is Responsible?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
FoE online
Trust and Accountability

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Technical Community, Asia-Pacific Group
Organizer 3: Intergovernmental Organization, Asia-Pacific Group

Speaker 1: Anju Mangal, Intergovernmental Organization, Asia-Pacific Group
Speaker 2: Babu Ram Aryal, Civil Society, Asia-Pacific Group
Speaker 3: Mamadou LO, Private Sector, African Group
Speaker 4: Angélica C, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 5: Walid Al-Saqaf, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

1. Is the current challenge of misinformation, its manifestation and affects, including reaction to misinformation similar in different nations, regions?

2. Are the initiatives (policy, technical, capacity building, others) taken so far by different stakeholders, especially the intermediaries and governments to curb spread of misinformation globally, regionally and within nations adequate?

3. Is it possible to moderate content through policies, while ensuring freedom of expression and privacy of users? Are there any best practices and approaches which may be adopted to counter misinformation being spread through messaging platforms and social media?

4. Is there any role of the multistakeholder process, other than Governments and intermediaries in the arena of content regulation?

Relevance to Theme: Various research done by organisations including the Internet Society, point that most internet users are losing their trust on the Internet. Misinformation, fake news, hate speech, issues of data privacy of users, the role of intermediaries are some of the greatest contributors to this dwindling trust deficit.
The BOF is aimed at discussing the issue of misinformation and its impact on nations and individuals, discussing the steps being taken as countermeasures so far; looking past the problems of misinformation in this digital age to coming up with ideas and solutions to counter the issue. The session also seeks to give participants an opportunity to share and explore their current concerns, discuss adequacy of the regulations being introduced by governments, steps taken by intermediaries and to think of new models and solutions that will help us create new ways of sharing information that is authentic and does not cause widespread harm to people in the future and helps building back the trust and accountability.

Key issues to be discussed:

1. The current challenge of misinformation, its manifestation and affects in different nations. The areas of convergence and divergence between nations in terms of the type of misinformation being circulated, the reaction to such misinformation and its effects.

2. Adequacy of the initiatives taken so far by different stakeholders especially the intermediaries, regulations introduced by governments to curb spread of misinformation globally and within nations. What more needs to be done.

3. Deliberate on Best practices and approaches which may be adopted to counter misinformation being spread through messaging platforms and social media; possible areas of regional cooperation.

4. Deliberate on the role of the multistakeholder process other than Governments and intermediaries in the arena of content regulation.

Relevance to Internet Governance: The Internet has ushered in new modes of communication and instant sharing of news. The compulsion of people to be up to date with news each minute has accelerated a surge in the spread of misinformation or 'fake news'.The elections of the US and Brazil have highlighted challenges in the flow of information. Creators of 'misinformation' are using the internet to operate, disseminate and influence communities, leading to even loss of lives. In India there have been incidents of mob lynching and killing of people based on false news.

Misinformation, fake news or disinformation has become a much discussed internet governance topic across the world, leading to discussions on intermediary liability, content regulation, role of governments etc.

Presently to mitigate the effects of misinformation, social media and messaging platforms have initiated several steps. Various governments across the globe such as EU, India, Nepal, Indonesia, New Zealand to name a few are drafting or contemplating new regulations for intermediaries to curb misinformation, that have raised concerns on the openness of the internet and freedom of speech.

Through the proposed BOF session we seek to understand whether the initiatives taken so far are adequate, while highlighting successful initiatives or what more needs to be done. Stakeholders from Asia: India, Nepal, Pacific Island, Europe, Latin America and Africa, would be invited to share the ongoing initiatives being taken by their governments, business and stakeholders to combat with the issue of misinformation; identify the best practices and then discuss if they can be replicated elsewhere to rebuild the trust over internet. The participants would also be discussing the role of the multistakeholder process other than Governments and intermediaries in the arena of content regulation.

Format:

Birds of a Feather - Auditorium - 60 Min

Description: Technology, especially the Internet has dramatically revolutionized many facets of our lives, both social and economic. It has not only driven innovation by ushering in new products and service, but also improved productivity in almost all economic sectors. For an average citizen, the internet has facilitated easier communication, enabled better engagement opportunities and helped in empowering them, it has democratised access to information, streamlined government service delivery and opened new markets for Indian businesses.

Social media and messaging platforms, which are widely used by people across the globe as a new mode of communication, owing to their ability to enable rapid and extensive exchange of information is a double edged sword. While social media and messaging platforms have helped civil society to mobilize people for a cause, there are also concerns alleging the disproportionate role of such platforms in influencing elections, including spreading false news, hate speech, religious, political and social misinformation. In fact, there have been reports of mob lynching and killing of people based on false news and such incidents have not only raised the alarm bells for law enforcement agencies, Government, but also civil societies and other stakeholder communities, thereby leading to a trust deficit online.

The proposed BOF will be an interactive session. During the discussion we aim to outline the major trends, initiatives taken so far by the online platforms, governments and other grass root communities and discuss on the best practices that can be adopted by different stakeholders to combat the challenge of

misinformation. Participants will be encouraged to share their concerns on the adequacy of the initiatives taken by different stakeholders and propose new models and solutions that will help enable sharing of information responsibly and rebuild trust of people on the internet.

Draft Agenda

1. Introduction to the subject by the moderator: 5 mins
2. Speakers share their country perspective: 20 mins
-Current challenges
-Adequacy of initiatives adopted
-Best practices observed and lessons learnt
-What more needs to be done
3. Open community discussion: 20 min
4. Summarizing the session and way ahead 5 mins

Expected Outcomes: At the end of the session we expect participants to get an insight on the,
• Existing challenges of misinformation and its manifestation in different regions
o Identify the common challenges across Global nations
o Emphasize the unique regional or national challenges if any.
• Best practices adopted by certain Intermediaries, nations or regions to overcome the challenges
• Areas which need reforms along with suggestions;
o Policy related to, improving content regulation and intermediary liabilities
o Engagement of other stakeholders
o Capacility Building initiatives
o Others

The participants of the session would subsequently be shared a summary report detailing the issues, best practices identified and recommendations based on the discussion for curbing misinformation and building trust back on the internet.

Discussion Facilitation:

To ensure the discussions are not tilted towards a particular economy, region or stakeholder, we will attempt to ensure the participation of all speakers are equally encouraged. We would also attempt to invite youth IGF representatives, local IGF participants into the discussion, besides community members from nations to attend and shared their perspectives.
The Moderator will be inviting comments and raising additional challenges for participants to respond and share their experience. We will strongly focus into including online participants equally in the discussion.
At the end of the session, we are looking into providing session's messages and conclusions for greater participation and understanding of the various aspects of the topic discussed.

Online Participation:

Interested community members from across the globe, who cannot be in Berlin in person would be encouraged to participate in the discussion remotely. Prior to the IGF we would be holding a series of discussions on the topic to gather more perspective of people and also in turn to encourage them especially the youth to participate remotely.
They would be informed through the various mailing groups, WhatsApp groups, social media groups about the event and the IGF remote participation links and process to connect.

Proposed Additional Tools: This workshop will rely on IGF support for remote participation and will also experiment with a variety of tools to bring in multiple views for the debate previously, during and after the presentation. Interactive document-building, intensive use of conversation in instantaneous social media such as Twitter, Facebook, Whatsapp or Weibo can be completed by warm-up sessions to the workshop with short video messages and notes.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #275 Framing encryption for a broader public

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Encryption

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Chris Riley, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Peter Koch, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Jenny Toomey, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

How can we promote public understanding of the use of encryption for security and safety in the context of government proposals for lawful access solutions?

Relevance to Theme: Encryption is a central component of securing our online communications and services that we use in our everyday lives, yet law enforcement agencies around the world are pushing for greater access to encrypted data and devices through backdoors and “lawful access solutions”. To inform democratic debate around this issue, we need to invest in improving global public understanding.

Relevance to Internet Governance: This is one of the most difficult internet governance topics faced around the world today, and although with legitimate aims such as protecting national security or public safety, often policy decisions are made in the wake of a crisis (a context known to result in bad policy) that might result in leaving the network less secure and more vulnerable. We need to be more proactive and engage and educate the public more to realize the vision of multistakeholder, democratic internet governance in this issue area.

Format:
Break-out Group Discussions - Flexible Seating - 90 Min

Description: - When people hear “encryption”, they often hear “you have something to hide”. Yet encryption is also an essential tool to secure our email, social networking, online banking, and increasingly all of our internet and Web activity from interception by criminals and bad actors. Encryption helps to secure government communications, enable secure transactions and private communications between users.
- We want to figure out how best to help people understand the positive role of encryption in their online lives, so they can be fully informed as citizens when their governments propose controversial laws meant to increase access to encrypted data and devices, which could compromise the security and privacy of their communications and data and weaken the overall security of systems that they use everyday.
- We propose setting up the issue and its challenges through an opening panel, and then facilitating breakout discussions to experiment with ideas and framing to help translate a very technical concept to a very broad public audience.
- We envision sending surveys around to attendees, possibly in advance or possibly after the session, to gather more input particularly from the youth, non-techie friends and family (i.e. not just the IGF attendee

type of person) on what kinds of ways of talking about encryption have the most impact.
- This workshop is organised by Mozilla, Internet Society and Ford Foundation.

Expected Outcomes: - Greater awareness of, and investment in, effective public education around encryption and its role in the internet ecosystem.
- Coalitions and partnerships to pool resources and drive bigger campaigns with more impact for bigger audiences.
- Follow up: Potentially, surveys and experiments run by attendees of the session to build a better global awareness of the state of play today and what sorts of educational campaigns have the most effect.

Discussion Facilitation:

We are planning to have facilitated breakout discussions for interaction and active participation during the session.

Online Participation:

We are planning to include remote participants into the discussion during the session with the help of remote moderators.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure

IGF 2019 WS #283 Transdisciplinarity for Internet Governance and Resilience

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Internet governance at local level
Resilience
Trust and Accountability

Organizer 1: Government, Asia-Pacific Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Asia-Pacific Group
Organizer 4: Civil Society, Asia-Pacific Group

Speaker 1: Seema Sharma, Government, Asia-Pacific Group
Speaker 2: Arnab Bose, Civil Society, Asia-Pacific Group
Speaker 3: Rohit Sen, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

1. What framework, methods and processes we need for better cooperation and collaborations among stakeholders (both offline and online) for effective internet governance and resilience at the local level
2. How can trust and accountability be restored?
3. How can cooperation and collaboration on national, regional and global levels help to increase cybersecurity?
4. What role should different stakeholders play in cybersecurity capacity building approaches?

Relevance to Theme: The proposed session would be able to answer four very important policy questions under the theme. The session also includes discussion on a live case study (design for sustainability

project- has a unique online and offline component, University of Delhi) to give real-time experience and understanding of the subject and to make the session a learning experience for everyone.

Relevance to Internet Governance: The session will be on how to achieve better cooperation and collaborations among stakeholders, needed framework, methods and processes to get effective internet governance and resilience at the local level.

Format:
Tutorial - Auditorium - 30 Min

Description: The proposed tutorial session will have three speakers and one moderator.
30 minutes session will be divided into three parts:-

1. Introduction and moderation for 2 minutes

2. presentation by the first speaker (5 minutes) on four policy questions raised (question no. 5).

3. Presentation on the live case study by the second and third speakers (4 minutes each, total of 8 minutes)

4. open discussion/question-answer session with all the participants (15 minutes) to collect the inputs/suggestions.

Expected Outcomes: The session will have four clear cut outcomes
1. Plausible framework, methods and processes for effective internet governance and resilience at the local level.
2. Methods to restore trust and accountability among local stakeholders/communities.
3. Methods and processes to attain better cybersecurity at the local level.
4. Role of different stakeholders in cybersecurity capacity building approaches.

Discussion Facilitation:

Before the start of the session, participants will be given the brochure to understand the context, subject, relevance and objective of the session. During the session, 15 minutes specifically will be allocated to the participants to interact/ask questions and share their experiences and point of views.

Online Participation:

Official online participation tool will be utilized by us to make the workshop session live. Back to India, students of the University of Delhi and O.P. Jindal Global University will join our session online.

Proposed Additional Tools: We will live stream our session through our facebook accounts using our mobiles to cover a large number of undergraduate students of University of Delhi and O P Jindal Global University.

SDGs:

GOAL 1: No Poverty
GOAL 2: Zero Hunger
GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 6: Clean Water and Sanitation
GOAL 7: Affordable and Clean Energy
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 12: Responsible Production and Consumption

GOAL 13: Climate Action
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Background Paper

Reference Document

IGF 2019 WS #287 Building a multistakeholder approach to secure crypto assets

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Cyber Security Best Practice

Organizer 1: Private Sector, Asia-Pacific Group
Organizer 2: Private Sector, Asia-Pacific Group

Speaker 1: Takanashi Yuta, Government, Asia-Pacific Group
Speaker 2: Shin'ichiro Matsuo, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Satish Babu, Civil Society, Asia-Pacific Group
Speaker 4: Louise Marie Hurel, Civil Society, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

Q1. Can we apply a multi-stakeholder approach to discuss governance and security of blockchain-based finance?
Q2. What kind of stakeholder is needed to discuss issues around crypto assets and blockchain-based finance?
Q3. How can we engage those stakeholders to the table?
Q4. How to provide a secure platform for customers(civil society)?
Q5. How does the government deal with crypto assets regarding financial regulation?
Q6. What can we learn from the existing forum or meeting such as IGF and ICANN?
Q7. Where do we make a mutual understanding of technologies and regulations?
Q8. How to make a regulation without hindering evolution of emerging technology?
Q9. What kind of issues do we have to prioritize?
Q10. What kind of working groups are formed based on the priority?
Q11. How can governments and regulators support?

Relevance to Theme: A secure financial platform is a crucial part of the world's economic activities. Crypto assets and blockchain technology could be a game-changing technology to achieve this.
Though many crypto assets custodians (e.g., virtual assets exchange) face security issues such as asset leakage, no common security consideration or operational practices are agreed among the entire ecosystem.
Therefore, security and safety to crypto assets and blockchain technology is awaited.

Relevance to Internet Governance: The Internet governance(I-G) community has evolved based on “a multi-stakeholder model” to tackle various issues of Internet resources. It is one of the success cases for people around the world to cooperate for solving problems. We propose to apply the same model for the governance of emerging technologies and society.

Crypto assets are well known as one of the use cases of "blockchain," emerging technology. Its market has emerged in these several years. Many custodians have been launched in Asia Pacific Area, in China, Russia, Singapore, Japan, Australia, Hong Kong, India, Indonesia, and Korea for example. Each county has started to discuss its regulation for the trading of crypto assets. Of course, we need the voice of users, civil society.

There are many concerns about the management of risks on crypto assets, such as Know Your Customer(KYC), Anti-Money Laundering(AML), Counter Financing of Terrorism(CFT) and leakage. Some of the custodians have been attacked by hackers, then they leaked customers' assets due to lack of security on their system. Though several industrial associations or technical alliances have been formed, there is neither global nor national/regional platform to discuss those problems by a balanced stakeholder yet.

Even though regulators and authorities are working on making a regulation for VASPs(Virtual Asset Service Provider), the rules and technologies of crypto assets and blockchain are rapidly changing by the discussion among the developers. As a result, the ecosystem couldn't assure that investor/consumer are protected from those incidents. We must have a multi-stakeholder process to address both technical and policy issues.

Therefore, we propose to apply the multi-stakeholder model to discussing crypto assets in this Internet Governance Forum where every stakeholder sit at the table together.

Format:
Round Table - Circle - 90 Min

Description: 【Intoroduction: 5min】
The moderator briefly introduces backgrounds of issues. We also plan to organize a similar workshop in APrIGF2019. Topics which discussed there will be shared in this part.
【Sharing each region or stakeholder's opinion: 48min】
Firstly, each expert introduces governance structure of crypto assets in their local region or stakeholder. Each expert will share their perspective of their interesting issues on the governance of crypto assets. Each pitch takes within 5 minutes. We do not use any slides here to encourage interactive discussion between participants. Every after expert' speaking, we have 5minutes for Q&A from audiences.
They expect present following topics below ;
- Common framework of security management of blockchain-based finance (crypto assets)
- Relationship between stakeholders
- Global collaboration (preventing regulatory arbitration)
- AML/CTF
【Making a recommendation: 30min】
The second half of the session will focus on making a recommendation for the global community to propose a multi-stakeholder forum to discuss issues around the regulation and security of crypto assets. A moderator will share a document sheet on a screen so that everyone can understand points which are discussed
The link will be shared with remote participants, too. At the end of this part, we will have a consensus by hamming to publish a document.
【Wrap up: 5 mins】
The moderator briefly describes discussion and our work in the session, then suggest some future work.

Expected Outcomes: Each participant including speakers and audiences brings their view. Then discussing and make a consensus on the requirements of the multi-stakeholder forum for crypto assets.

The outcome of this session will be a recommendation to launch a multi-stakeholder forum to discuss security, regulation and technical issues on crypto assets and blockchain-based finance. We will publish a recommendation for a global society. We also plan to share the URL of the document on the IGF Webpage(workshop page). We will also encourage participants of this session to share the document with local communities.

Discussion Facilitation:

Regarding online moderation, we prepare one moderator to help them.
Online participants can join us via WebEx. We accept both text message and call to take the floor.
- Text message: Participants can share their opinion without worrying about the network connection. An online moderator will speak instead of them.
- Call: They can join the session with the WebEx system, however, we may recommend using a text message if your/our Internet connection is not good enough.
To facilitate an interactive discussion, we will prepare the Open mic in the center of the room. We expect every participant freely shares an opinion or asks a question to experts.

Online Participation:

Our online moderator will use WebEx chat to ask for questions or opinions during the workshop.

Proposed Additional Tools: Use Twitter, Facebook to catch up the ideas and opinions from remote participants.

SDGs:

GOAL 1: No Poverty
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #289 Development of Technical Internet Policies and Social Values

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Internet ethics
Internet Protocols
Internet Resources

Organizer 1: Government, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Western European and Others Group (WEOG)
Organizer 3: ,
Organizer 4: Government, Western European and Others Group (WEOG)

Speaker 1: Constanze Buerger, Government, Western European and Others Group (WEOG)
Speaker 2: jin yan, Private Sector, Western European and Others Group (WEOG)
Speaker 3: Tahar Schaa, Government, Western European and Others Group (WEOG)

Policy Question(s):

Which cultural values are defining your internet usage? What role do Internet protocols play in the fight against cyber attacks? What role should different stakeholders play in cybersecurity capacity building approaches? Trust and Accountability: How can trust and accountability be restored? How can globally accepted standards be developed?

Relevance to Theme: Only ensured participation of all stakeholders of the society makes a sustainable internet development possible. This prevents the divide of the internet into several parts and several other negative issues.

Relevance to Internet Governance: Strengthen the policy development in the internetorganizations like the NROs and the IETF is a direct positive effort for a biased and included Internet Governance. The role of governments itself and the importance of civil society and private sector is important to this.

Format:
Birds of a Feather - Auditorium - 60 Min

Description: Internet defines todays life in every level. Therefore the way policies for Internet Resources and technical standards are developing while participation is ensured is essential.
Countries are legitimate internet users and stakeholders themselves. Although In the policy development process, we have a standard stakeholder role .
This multi stakeholder approach is new task for the countries to take care about, to ensure the participation and sense full engagement of everyone in the internet.

Expected Outcomes: Creating awarenes for the democratic policy development processes. Strengthen the participation in policy development processes. Give an example to engage for other countries.

Discussion Facilitation:

After an impulse presentation feedback and opinoins are ask directly to certain persons of the audience and used to start an interactive discussion.

Online Participation:

Online comments will be read for all in the audience and included in the discussion.

SDGs:

GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions

Background Paper

Reference Document

IGF 2019 WS #290 The future of the liability regime of online platforms

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
FoE online
Hate Speech
Human Rights

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Rotert Michael, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Jan Penfrat, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Aleksandra Kuczerawy, Technical Community, Eastern European Group
Speaker 4: Arzu Geybulla, Civil Society, Eastern European Group
Speaker 5: Wafa Ben-Hassine, Civil Society, African Group

Policy Question(s):

Recent proposals and rules around the world are undermining the limited liability protections which have under-pinned the Internet in recent decades. Europe, for instance, has adopted a Copyright Directive with mandatory content filtering mechanisms. The EU is expected to reopen the e-Commerce Directive. In the USA, SESTA/FOSTA entered into law in April 2018. In India, the government's draft intermediary guidelines introduces short timeframes to remove content. Australia explicitly refrained in 2018 from expanding liability protections outside of a narrow category of intermediaries. Are existing rules fit for purpose? What are the broader societal impact of new rules, e.g. on fundamental rights and democratic principles such as the rule of law?

Relevance to Theme: The limited liability regime applied to online intermediaries is the legal foundation of freedom of expression online, access to information and of the economic development of the digital sector. However, recent laws and policy proposals tend to change this regime as a way to fight against hate speech, terrorist content online and more generally against violence and sexual abuse in the online environment. Discussions on the liability regime of online intermediaries should take place at regional and global levels to ensure consistency and stability, to address the legitimate concerns caused by illegal content online and to protect access to information and freedom of expression online.

Relevance to Internet Governance: Legislations and policy proposals aiming to increase the liability of online intermediaries would profoundly impact the evolution and use of the Internet. It is vital for governments, companies and citizens' representatives to ensure a balance between the fight against illegal content online, citizens' fundamental rights and companies' obligations.

Format:
Panel - Auditorium - 60 Min

Description: Agenda

1. Highlight current trends on online intermediaries' liability reforms (20 min): More and more countries are discussing and/or adopting legislation undermining the limited liability regime of online intermediaries, as understood for the past 20 years. We will hear the views from representatives from Europe and Brazil on such discussions/legislations, raising also examples from recent discussions in India.

2. Looking ahead on where such discussions should go (20 min): Building on the state of play described in the first part of the panel, the panellists will then discuss the different approaches taken and which direction, in their opinion, such discussions and legislations should take.

3. Q&A session with the audience (20 min).

Expected Outcomes: (a) Recognise that the limited liability regime of online intermediaries is increasingly challenged across the world.
(b) Contribute to on-going and future multilateral and bilateral dialogues to ensure a balance between the fight against illegal content online, citizens' fundamental rights and companies' obligations.

Discussion Facilitation:

Short two to three minutes presentations made by the speakers will open the discussions. The remaining time of the workshop will be allocated to open discussions, with on spot and online participants encouraged to present their views and possible solutions during the last 20 minutes of the panel.

Online Participation:

Online and onsite participants will be able to ask questions and participate to the debate during the last third of the panel.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #292 The Philosophical Underpinning of Cloud Native Governments

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Democratic Values
Trust and Accountability

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Philipp Mueller, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Mueller Parycek, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Arturo Franco, Private Sector, Latin American and Caribbean Group (GRULAC)
Speaker 4: Miksch Jennifer, Government, Western European and Others Group (WEOG)

Policy Question(s):

How does the idea of "cloud native" impact constitutional, cultural, and procedural dimensions of democratic governance? What are the possibility spaces, what are risks? What are the experiences of different states that have gone cloud native?

Relevance to Theme: The cloud native concept as it is being implemented in governments worldwide is having an impact on global resilience.

Relevance to Internet Governance: in a world of cloud, artificial intelligence, and the internet of things, we need to broaden the questions on internet governance and openly raise geopolitical questions on how to think in decades and centuries.

Format:
Birds of a Feather - Auditorium - 60 Min

Description: The internet and its corollary technologies such as cloud, artificial intelligence, and the internet of things have had the biggest impact on fundamental questions of the governance of government, since the writing of Thomas Hobbes on the contractual foundation of the sovereign. In the workshop we will reflect the opportunities and challenges governments are facing in a world that has gone cloud native. Participants will be government officials from the global south and north, academics, and technologists.

Expected Outcomes: A comparative government perspective (in written form)
guidance for governments planning to implement cloud
an exchange of ideas

Discussion Facilitation:

the moderator will frame the session, we will do short provocative interventions, then engage in the group and with the audience.

Online Participation:

moderated questions.

Proposed Additional Tools: twitter and social media in prep, during, and after the session

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities

IGF 2019 WS #295 Public diplomacy v. disinformation: Are there red lines?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
FoE online
Trust and Accountability

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Eastern European Group

Speaker 1: Iskra Kirova, Civil Society, Eastern European Group
Speaker 2: Marilia Maciel, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 3: John FRANK, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Felix Kartte, Intergovernmental Organization, Western European and Others Group (WEOG)

Policy Question(s):

Norm on preventing interference in electoral processes: How do we define foreign interference? Where are the red lines between public diplomacy and election interference? Are there situations in which foreign election interference and corresponding use of cyber-enabled tactics such as disinformation be deemed acceptable? How can disinformation be used for nefarious and legitimate purposes? What international legal frameworks govern election interference and disinformation? Finally, what can we do to mitigate these threats in order to prevent interference in electoral processes?

Relevance to Theme: Security and safety are prerequisites to economic growth and a healthy digital environment beneficial to all. To achieve security and safety requires having a set of commonly understood and followed rules of behavior in the digital space which guide actions and punish deviations from those rules. The Paris Call for Trust and Security in Cyberspace, which has been signed by over 500 entities (governments, civil society and industry organizations) worldwide, calls on the world to work together to "prevent interference in electoral processes." However, to make progress on norms for security and safety, including noninterference in elections, we must first look to defining the scope and terminology of election interference.

Relevance to Internet Governance: Norms of behavior in cyberspace are a critical component to governing our actions online. The increased trend of interference in elections over the past decade, aided by new technologies, has led governments, industry and civil society actors to call for new norms against the interference in elections. This panel seeks to deep dive into one specific aspect of election interference, regarding the legitimate and illegitimate use and manipulation of information to influence an election.

Format:

Round Table - Circle - 60 Min

Description: Cyber-enabled threats to democratic processes continue to be a concern around the world. In 2018, half of all advanced democracies holding national elections had their democratic processes targeted by cyber threat activity, which represents a three-fold increase since 2015 and a trend that we expect to continue in the coming year.

Recognizing this threat and increasing trend, many governments, civil society groups and industry have sought to take action through underscoring the need for action in diplomatic dialogue and intergovernmental fora, such as through the Paris Call for Trust and Security in Cyberspace and the 2018 G7 Charlevoix Commitment on Defending Democracy from Foreign Threats. But to make progress on defending democracy and protecting election integrity requires better understanding the core definitions around these issues.

Foreign intervention in democratic elections, whether to promote democratic values or to achieve opposite goals, can be seen as part of those foreign policy tools – ranging from diplomacy through negotiations, provision of foreign aid or imposition of economic sanctions, etc. – that countries' have at their disposal. Beyond great powers, regional and international organizations have a well-documented history of influencing third countries' governments in order to promote democratic values – namely, greater peace, prosperity, and pluralism.

On the other hand, malicious actors seeking to interfere in the political climate or election of another country for nefarious purposes is also increasing in scale and impact given the development of technological tools. For both malicious actors and legitimate actors seeking to promote democracy or a particular political agenda, many of the tactics used can look similar: from disseminating rumors (false or true) to damaging rival candidates credibility, public threats or promises, public statements in support of candidates, provision of campaign funds, or increasing foreign aid or other types of assistance.

This panel (full title) "Realpolitik foreign policy or manipulation of sovereign democratic processes: where's the red line?" is intended to facilitate a discussion around foreign interference and the use of disinformation. The Paris Call for Trust and Security in Cyberspace, which has been signed by over 500 entities (governments, civil society and industry organizations) worldwide, calls on the world to work together to "prevent interference in electoral processes." While foreign election interference is not a new phenomenon, traditional tactics can now be achieved at a much greater scale with the help of new technologies. This is why it is critical to make progress in understanding the norms and rules of the road in this space.

Throughout the course of the roundtable, experts and roundtable participants will answer the following questions: How do we define foreign interference? Where are the red lines between public diplomacy and election interference? Are there situations in which foreign election interference and corresponding use of cyber-enabled tactics such as disinformation be deemed acceptable? How can disinformation be used for nefarious and legitimate purposes? What international legal frameworks govern election interference and disinformation? Finally, what can we do to mitigate these threats in order to prevent interference in electoral processes?

Format

- Overview of election interference trends and threats (5 minutes)
- Context setting on public diplomacy tools in the information space (5 minutes)
- Case study deep dive (i.e. Ukraine, South America) (10 minutes)
- Moderated discussion of roundtable questions (25 minutes)
- Open mic session (10 minutes)
- Conclusion and next steps (5 minutes)

Expected Outcomes: Very few, if any discussions around disinformation and election interference have focused on the idea of defining norms of behavior around what is acceptable activity in this space. In order to make progress on the commitments of multistakeholder agreements such as the G7 Charlevoix Commitment on Defending Democracy from Foreign Threats or the Paris Call for Trust and Security in Cyberspace, we must be able to accurately define the issue and then agree as an international multistakeholder community on what is permissible behavior. This panel is intended to be a starting point to make progress on this pillar and the findings of the discussion will be used in follow-up roundtables across the future gatherings of the "Friends of the Paris Call" or other initiatives designed to make progress on cybersecurity norms against the interference of elections and democratic processes.

Discussion Facilitation:

An open mic session follows the main session to enable the audience and remote participants to join the conversation and present their experiences, opinions, suggestions, etc., on how to move the debate forward. Audience discussants will either queue at their stakeholder-assigned mics, or the panel rapporteurs will bring the mics to discussants, and rotate, with online participants having their own equal queue.

Online Participation:

We will have two online moderators to assist with the online conversation. To broaden participation, social media (Twitter and Facebook) will also be employed by the on-line moderators who will be in charge of browsing social media using a dedicated hashtag.

Proposed Additional Tools: In order to broaden the conversation before, during and after this roundtable we would like to set up a dedicated Microsoft Teams channel in which interested participants can contribute to the discussion by adding questions, sending news articles and following up with experts. During the session Teams can be leveraged for its accessibility features (such as Translator, screen viewer, dictation) to enable those with disabilities to contribute to the conversation.

SDGs:

GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #307 Transparency and Control for the Internet of Things

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Cyber Security Best Practice

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Chris Kubecka, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Estelle Massé , Civil Society, Western European and Others Group (WEOG)
Speaker 3: Sunil Abraham, Civil Society, Asia-Pacific Group
Speaker 4: Thomas Schildhauer , Civil Society, Western European and Others Group (WEOG)
Speaker 5: Maarten Botterman, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

Review of the current landscape: What are the best existing frameworks that can help drive security standardization for the consumer Internet of Things?

How do we empower users to make choices about the world of devices around them?
- How should / can users understand their threat models?
- How can users make decisions about security capabilities? Can they assume certain risk? Must there be certain minimum requirements?
- How do users make decisions about product functionality? What options for “dumb” devices? What can users know / control about sensors and device capabilities?
- For devices that are not apparent to users (or under their control), how can users understand them and interact with them?

What are the most promising mechanisms to drive international standardization across stakeholders and supply chains?
Can we agree on alignment around certain aspects of devices where standardization makes sense?
- Device type? (e.g., security camera, television, home appliances)
- Sensor type? (e.g., microphone, camera, accelerometer, thermometer)
- Type of data collected? (e.g., personally identifiable data, environmental data, medical data) And do you go by device or sensor capabilities or intended use?

Relevance to Theme: The number of Internet-connected devices now exceeds the world’s population. And by 2021, Gartner estimates that the number of Internet-connected devices will triple to 25 billion. It is perhaps unsurprising that the volume and sophistication of IoT threat has consequently grown to identify and exploit vulnerabilities. And while there are embryonic efforts to foster a marketplace for safe and secure IoT products, those efforts require international consensus, standardization, and commitment across a broad universe of government and industry stakeholders.

A recent report found that internet of things attacks doubled between 2017 and 2018. Many of the attacks rely on weak/default credentials, and unpatched vulnerabilities.

We would aim to build off of the work from last year's convening:
https://www.intgovforum.org/multilingual/content/igf-2018-dc-internet-of...

Relevance to Internet Governance: Securing the IoT marketplace will require the participation and collaboration of stakeholders across the globe. Although many of these devices are purpose-built to operate in a local environment, their connectedness means that they can often be accessed and/or controlled remotely. If not secured, some devices may be used to improperly collect and share data, or may be used as bots by an attacker.

To address these issues, we must consider global supply chains in global market and how the diverse stakeholders in the ecosystem can organize, monitor and govern their security/quality standards. Standards and protocols that provide baseline security for IoT consumers should apply regardless of where devices are made or where they are used. Further, the interconnected nature of global commerce means that the adverse effects of security vulnerabilities in Internet-connected devices will not be confined to particular countries and regions. Thus requiring a transnational multistakeholder framework of incentives and governance practices.

Work on national-level solutions might help to pioneer the state of the art for Internet governance, but experiences have to be “internationalized” to ensure the development of a long-term, safe and secure IoT marketplace.

Format:
Birds of a Feather - Auditorium - 90 Min

Description: Intro to challenge and opportunity (per policy questions above)
- Overview of current state of the art (e.g., The Digital Standard, other frameworks)

- 2 minute overviews by speakers to “pitch” particular frameworks.

What form of scheme?
- Some breakout to discuss: Labeling? NRTL model?
- Some breakout to discuss:: What attributes of devices need to be regulated (see 5 above)

Lead group to consider which of the existing frameworks makes the most sense to pursue.
- Discussion / Agreement of next steps

Expected Outcomes: Organizers would seek self-nominations from participants to integrate with existing IoT security framework efforts and assist them with coordinating input and bootstrap a multistakeholder community of practice (potentially connected to the IGF IoT Dynamic Coalition).

Discussion Facilitation:

As noted above, we will feature breakouts as well as an opportunity at the end for groups to weigh in on a recommended set of next steps.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 9: Industry, Innovation and Infrastructure

IGF 2019 WS #310 DOH! DNS over HTTPS explained

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Domain Name System
Encryption
Internet Protocols

Organizer 1: Technical Community, Western European and Others Group (WEOG)
Organizer 2: Technical Community, Western European and Others Group (WEOG)
Organizer 3: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Byron Holland, Technical Community, Western European and Others Group (WEOG)
Speaker 2: Geoff Huston, Technical Community, Asia-Pacific Group
Speaker 3: Patrik Fältström, Technical Community, Western European and Others Group (WEOG)
Speaker 4: Suzanne Woolf, Technical Community, Western European and Others Group (WEOG)
Speaker 5: Mariko Kobayashi, Technical Community, Asia-Pacific Group

Policy Question(s):

How does concealing DNS queries within an encrypted channel affect enterprise network management?

What is the impact on law enforcement?

Are there benefits of DOH for the internet ecosystem (e.g. infrastructure, robustness, trust) that extend beyond privacy?

What challenges does DOH pose to the present namespace?

What challenges does browser-based DNS resolution pose to personal privacy?

Relevance to Theme: DOH is a DNS resolution protocol designed to increase user privacy and security by eliminating the ability to intercept and manipulate DNS data. DOH does not need to query public DNS infrastructure to resolve a domain name, instead forging an encrypted end-to-end connection between the end user's device and a web server.

The confidentiality of DNS requests afforded by DOH prevents DNS hijacking and spoofing. This also makes it more difficult to share DNS data with third parties (such as governments of corporations.)

However, DOH can be enabled within a browser without the user's explicit knowledge or permission. This raises an entirely new set of privacy issues relating to user data being directed to third parties in a manner that is invisible to the user.

Relevance to Internet Governance: The increased privacy from public DNS infrastructure that is afforded by DOH is not without criticism.

Some security and privacy experts object to DOH on the basis of operational risks to network operators, its compatibility with privacy legislation, and the increased power of browser developers and their preferred DNS resolvers over internet users.

DOH represents a fundamental shift in internet architecture and challenges the status quo hierarchical namespace. The protocol is a topic of hot debate between stakeholders who currently operate different pieces of the DNS, as well as network administrators who would lose the ability to manipulate traffic, and law enforcement agencies' ability to investigate based on DNS traffic.

Format:
Birds of a Feather - Classroom - 90 Min

Description: DNS over HTTPS (DOH) is a DNS resolution protocol designed to increase user privacy and security by eliminating the ability to intercept and manipulate DNS data. DOH does not need to query public DNS infrastructure to resolve a domain name, instead forging an encrypted end-to-end connection between the end user's device and a web server.

This BoF aims to explore the emergence of the DOH protocol and the associated policy issues in a manner that is accessible for all stakeholders of technical and non-technical backgrounds.

With the guidance of technical and policy professionals from various stakeholder groups, BoF participants will discuss the state of the latest implementations, policy questions, and challenges related to running DNS over HTTPS.

Expected Outcomes: BoF participants will learn how DNS over HTTPS functions and how it departs from the current DNS architecture
BoF participants will discuss different perspectives of DNS over HTTPS and the policy issues associated with its implementation

Discussion Facilitation:

The workshop will be organized as a BOF. Led by the moderator, a short presentation on the latest developments on DOH will presented and key questions presented for discussion and dialogue.

The moderator and remote participation lead will seek to promote and encourage a facilitated dialogue among the subject matter experts, invited experts in the audience, and those participating virtually.

Knowing there is considerable interest in the topic, efforts will be taken to record comments and/or video interventions from experts whose schedules do not make it possible for them to be present the date/time of the session.

In addition to the background documents and papers that will be prepared ahead of the IGF, additional articles of interest, commissioned blogs, reference materials and social media conversations will be published and distributed ahead of the workshop.

Online Participation:

Knowing there is considerable interest in the topic, efforts will be taken to engage experts virtually whose schedules do not make it possible for them to be present the date/time of the session.

Proposed Additional Tools: Knowing there is considerable interest in the topic, efforts will be taken to record comments and/or video interventions from experts whose schedules do not make it possible for them to be present the date/time of the session.

In addition to the background documents and papers that will be prepared ahead of the IGF, additional articles of interest, commissioned blogs, reference materials and social media conversations will be published and distributed ahead of the workshop.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure

Reference Document

IGF 2019 WS #314 Where now? Navigating cybernorms at the UN First Committee

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
International Norms
Cyber Attacks
Resilience

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Wolfram von Heynitz, Government, Western European and Others Group (WEOG)
Speaker 2: Olaf Kolkman, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Deborah Brown, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

What are the links between cybersecurity, international peace and security and roles and obligations of states when it comes to human rights?
What can the First Committee processes achieve? How can they work together? How do they relate to other cybernorms discussions?

Relevance to Theme: The year 2019 sees the launch of two high-level, parallel processes within UNGA's First Committee that relate to cybersecurity: An Open-Ended Working Group and a Government Group of Experts (GGE). Both processes will consider how to promote cybersecurity by considering what defines responsible behaviour of states in cyberspace. These discussions therefore closely relate to the security, safety, stability and resilience of the internet.

Relevance to Internet Governance: Cybersecurity remains one of the most pressing issues in internet governance. Many of the policy discussions at the global level relate to the appropriate role of different

stakeholders in ensuring cybersecurity, which is a key question in internet governance. Although there is widespread acknowledgement of the importance of an inclusive and multistakeholder approach to ensuring the security, stability and resilience of cyberspace, these discussions remain largely closed and securitised. There continues to be a lack of agreement on many key issues, including on what the duties and obligations of state actors are and how to enforce them, and how to interpret existing principles of international law, such as sovereignty, as well as the place of international human rights law in these discussions. These discussions therefore directly relate to a range of internet governance issues, including about the "norms, principles, and rules" that should govern the internet.

So far, the discussions within the First Committee, including most importantly the Group of Government Experts (GGE) have been important and have influenced other global cybersecurity policy processes. In the meantime, since the last GGE report (2015), many other bilateral, multilateral and multistakeholder efforts have contributed to the cybernorms discussion. At this new stage in the First Committee discussions, new approaches to the global governance regime for cybersecurity may be considered - particularly if the OEWG develops recommendations for a global treaty. Therefore, this is a critical juncture to assess and input into discussions at a forum which could fundamentally impact the governance of the internet.

Format:
Panel - Auditorium - 60 Min

Description: This workshop offers an opportunity to share information on the First Committee processes, discuss their progress so far and have an interactive discussion which it is hoped will feed directly into the processes. The end aim will be to facilitate a discussion among the international multistakeholder community on the OEWG and the GGE processes hear from the IGF community what they should address, and will therefore offer an opportunity to make these processes more open, inclusive and transparent. The IGF workshop will be held after the first OEWG substantive session (in September 2019) and just prior to the the GGE session in New York (December), as well as the first multistakeholder intersessional in December. It would therefore come at an important juncture in the discussions.

The workshop would also act as a follow-up to a session at the 2019 edition of RightsCon in Tunis, where stakeholders will also gather to discuss the processes and opportunities relevant to the First Committee processes.

The session will begin with information-sharing from the panelists on the processes and the discussions so far.

The panel would respond to three main questions:
1. What are the OEWG and the GGE and what are their aims?
2. Considering the agendas of the two processes, what should the outcomes be?
3. What are the challenges and opportunities for non-governmental engagement, and civil society engagement in particular?

The moderator will then facilitate an open and interactive discussion with participants so as to gather reflections on key issue areas and concrete proposals to feed into the processes. Finally, further opportunities for non-government engagement following the session will also be discussed and shared.

The process for constructing cybernorms shapes their content and it is therefore expected that the discussions in this workshop will be able to feed into the discussions of the GGE and OEWG, and will act as a reference for views from a multistakeholder grouping of the issues on the agendas of both processes. The IGF offers a unique space as a multistakeholder forum, connected to the UN to have these discussions. In this sense, the open, interactive nature of the IGF will promote more inclusivity into the First Committee processes.

Expected Outcomes: 1. Broader understanding of the global cybersecurity discussions
2. Concrete recommendations and suggestions to feed into two existing, high-level UN processes related to cybersecurity by a range of stakeholders

Discussion Facilitation:

One of the primary aims of the session is to gather perspectives on discussions related to cybersecurity in the UN's First Committee which directly impact internet users and the IGF community but which are unfortunately largely closed to non-governmental stakeholders. Therefore, following brief introductory remarks from the panelists, the audience will be offered ample time to input and will be asked to offer their perspectives on the First Committee processes.

Online Participation:

The onsite moderator will turn frequently to take questions from the remote participants and the online moderator will pose questions from remote participants to the panel during the interactive discussion.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #316 Emerging perspectives on the Internet Exchange Points

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Internet kill switch
Internet Protocols
Internet traffic

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Technical Community, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Latin American and Caribbean Group (GRULAC)
Organizer 4: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Patricia Vargas, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Olga Cavalli, Government, Latin American and Caribbean Group (GRULAC)
Speaker 3: Enrico Calandro, Civil Society, African Group

Policy Question(s):

1. What is the role of the IXPs in facilitating Internet connectivity?
2. What are the essential aspects local legislations include when they regulate IXPs?
3. How is the perspective of the private sector about IXPs?
4. What are the policies of hybrid and democratic regimes regarding IXPs when considering a form of extreme government control, like an Internet kill switch?

Relevance to Theme: This panel intends to cover at least two relevant sub-themes of the IGF, related to the areas of stability and resilience of the Internet infrastructure, and at some extent, digital inclusion.
Internet Exchange Points (IXPs) are part of the physical layer of the TCP/IP protocol, and their function is to allow Internet networks to interconnect directly or exchange traffic. In this way, IXPs are infrastructures that facilitate and transfer information among Internet service providers (ISPs) and interconnect national and international networks. The more IXPs a nation-state has, they improve the quality of the Internet activity (in and out of the territory of that nation-state) and reduce the costs of the service.

In recent years, different stakeholders of the Internet highlighted the importance of the IXPs to guarantee the stability of their infrastructure and to keep the Internet packets within the national borders of the territory of individual nation-states. This characteristic allows preserving the confidentiality of the information the different national stakeholders handle through the Internet and keep the stability of the Internet ecosystem.

Relevance to Internet Governance: The OECD has established that an essential characteristic of the IXPs is that their design is based on voluntary contractual agreements. In fact, most IXPs at a worldwide level are privately owned and built by private organizations, but provide stability in the Internet connection for all Internet stakeholders (governments, citizens-Internet users, corporations, international organizations, etc). The exchange of traffic through an IXP is possible because of the routing configurations by the Border Gateway Protocol (BGP).
In this context, IXPs become a critical element for the resilience and stability of the Internet, but also an aspect of facilitating and enabling Internet connectivity. Being this the case, they are also an element to analyze when considering an Internet kill switch, the most extreme form of government control over the Internet.

Format:
Round Table - U-shape - 90 Min

Description: The moderator will begin the session by presenting and introducing the discussion (2 minutes). Then she will give the floor to the speakers who will offer their perspective and personal experience according to the sector they represent (academia, civil society, the private sector, government). Each speaker will have 15 minutes for their presentation. The Q/A session will take around 25 minutes and finally the conclusion (3 minutes).
The speakers will:
1. Provide an overview of IXPs functionality and their importance to facilitate the traffic of the Internet packets
2. Explain local legislations attempts to control the IXPs networks activity and their effect over the private sector
- At least two speakers will provide an overview of IXPs functionality from the private sector perspective. This is a crucial point because, as mentioned before, IXPs all over the world are mostly privately owned.
3. Explain how nation-states attempted to recognize legally a form of government control, known as "Internet kill switch," (shutdown of the entire Internet within the borders of a nation-state) and why IXPs are relevant in this context.
4. Explain how the stability IXPs provide within the Internet ecosystem can prevent Internet kill switches

Expected Outcomes: It is the purpose of this panel to explore the ways IXPs facilitate connectivity among multiple international networks and, with this goal in mind, to analyze local legislations attempts that try to control IXPs and their impact over the private sector.
The listed policy questions address two problems, connectivity and of government control policies over the Internet infrastructure.
Up to this point, most of the academic and non-academic work is based on the importance and role of the ISPs, while IXPs have been analyzed mostly from a technical perspective, but not from a policy one.
This project attempts to bring back into the debate the role and multiple advantages of the IXPs as one of the main elements that facilitates the end-to-end principle and keeps the integrity of the Internet data packets and the Internet ecosystem.

Discussion Facilitation:

We are planning to have a round table of at least four speakers, of which at least they will present five topics for debate.
The order will be opening of the moderator (presentation of the workshop) - each speaker makes a presentation- the moderator calls for the Q/A session. Finally, the moderator will call for the last comment and will provide the final remarks.

Our onsite moderator is an experienced member of academia that has been and participated in multiple panels at past IGFs. Our online moderator, a member of the private sector, has been the organizer of a workshop in previous IGF as well.
Online participation will enrich the debate, and we intend to have diverse involvement from all over the world.
To increase the exposure and impact of this workshop, we will use both platforms, twitter, and Facebook, to facilitate coordination and communication. Additionally, we will use the official participation channels. Our moderator will distribute remote and local participation of the speakers and the audience.
During the Q/A session, questions will follow queuing, and the moderator will try to group similar items so that more issues can be addressed and no single topic or speaker or group of speakers monopolize the debate.

Online Participation:

We expect to spread the news about our workshop to have active participation in line, and our online moderator is qualified to moderate the interventions.

Proposed Additional Tools: If possible, we expect to transmit the workshop by Facebook Live/Live Video Streaming and Instagram. The use of these platforms would help to increase participation even in countries where connectivity is low, or people only have access to the mentioned platforms.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities

IGF 2019 WS #318 Legislation for Fake News

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
Jurisdiction

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group

Speaker 1: Bruna Santos , Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Olumuyiwa Caleb Ogundele, Civil Society, African Group
Speaker 3: Nadia Tjahja, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

1) Can fake news regulations be successful in curbing misinformation without threatening the rights and safety of journalists?
2) Should a country's legislation for fake news apply to international organisations and media houses with regional headquarters in the country?
3) How can checks and balances be built into legislation to protect the freedom of expression?
4) What are the kinds of legal regulations already in place, and to what extent are they successful in curbing the issue of fake news without infringing on the right to free speech?
5) How can legislation be leveraged to create an effective but fair co-regulation model?

Relevance to Theme: Any legislation surrounding the regulation of media has the potential to be misused. Fake news is still a relatively new issue and many nations, particularly in the global south, are still struggling

to define the parameters of their conversations. Thus, rushed and vague policy decisions can undermine the safety and rights of dissenters - where laws can be manipulated to adversely affect the freedom of expression.

Relevance to Internet Governance: This session looks at laws relating to the regulation of new media in light of the increasingly prevalent issue of fake news and misinformation. Many countries have already passed legislation which has resulted self-censorship, and has been used for the unjust imprisonment for journalists. This session will explore the intricacies of these policies, and the different regulation approaches available to best serve the interests of the people.

Format:

Break-out Group Discussions - Round Tables - 60 Min

Description: The topic of legislation around fake news will be introduced with a short presentation giving background and context to the participants. This will cover how countries across the globe are responding to the threat of misinformation. It will also include a few case studies where legislation is currently being debated.

In order to use time and the skills of the participants efficiently, this session will use the "Break-out Group Discussion" format to pose the policy questions to each group. These discussions will be summarised at the end of the session which will help identify common threads and policy suggestions.

Expected Outcomes: This session seeks to understand the strengths and weaknesses in fake news legislation. Through the workshop format, the session will use the experiences, knowledge and collaboration of the participants to yield some insights into what constitutes sound legislation that cannot be manipulated to undercut democracy and democratic activities.

Discussion Facilitation:

The session relies on interaction and participation of members within the small group discussions. Each discussion will be a collaborative effort to yield solutions and insights that can be shared with the rest of participants at the end of the session.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #321 The end-user's perspective on the 'internet of trust'.

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

Democratic Values
Resilience
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Technical Community, African Group

Speaker 1: Serge parfait Goma, Civil Society, African Group
Speaker 2: Htaike Aung Htaike, Civil Society, Asia-Pacific Group
Speaker 3: Gabriel Ramokotjo, Civil Society, African Group

Policy Question(s):

➢ From a personal experience, what do you consider as key components of an 'internet of trust'?
➢ How do the actions of stakeholders influence your experience of the internet in terms of security, safety, stability and resilience?
➢ What are your options for digital connection when working and living in an environment where the internet is not secure, safe, stable or resilient, e.g. in countries where internet shutdowns are regularly applied, and areas where there is limited coverage?
➢ What or who do you consider as the biggest threats to internet security, safety, stability and stability? How does the lack of a stable, secure, resilient safe internet affect human rights in general, and free expression in particular?
➢ What are your recommendations for building an 'internet of trust'? Are the particular groups whom you think should benefit from targeted actions to improve their experience in terms of the stability, security, resilience and safety of the internet?

Relevance to Theme: The session will explore the internet's safety, security, stability and resilience from the end-user's perspective. It will further provide insight into how to achieve an 'internet of trust' from a perspective that should be most important, that of the end-user.
The IGF provides an opportunity for diverse representation at the session, which will reflect in the discussion and engagement.

Relevance to Internet Governance: The end-user should be the most important consideration in the internet ecosystem and the development of ICT policies. The session is relevant to IG because it highlight's the end-user's experiences and perceptions of the internet in relation to safety, security, resilience and stability. It will provide important insights for policy makers, researchers, and those tasked with the safety, security, resilience and stability of the internet.

Format:
Round Table - Circle - 60 Min

Description: The roundtable discussion is aimed assessing the end-users experience of the internet in relation to security, safety, resilience and stability. To encourage free expression, the facilitator will set an informal tone.
The facilitator will make a brief introduction to the session and discussion starters, after which any of them are free to share their view on the theme. Each speaker has a maximum of two (2) minutes speaking time. The facilitator will conclude the session with key points that emerged from the discussion.

Expected Outcomes: ➢ Diverse perspectives on the 'internet of trust' in relation to its security, safety, stability and resilience for the end-user.
➢ Increased awareness on opportunities that can be harnessed, and threats that can be mitigated in regards to the end-user and their experience with the internet.
➢ End-users provide key recommendations from on the building of an 'internet of trust' within the context of safety, security, stability and resilience.

Discussion Facilitation:

The facilitator will set an informal tone to encourage free expression. Key question will be asked to stimulate discussion, while the discussion starters will set the tone by sharing their views at the initial phase.

Online Participation:

Remote participation is a critical component of this discussion.

Proposed Additional Tools: Social media

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 12: Responsible Production and Consumption
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #328 Multistakeholder Models for Online Content Moderation

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
FoE online
Hate Speech
Human Rights

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: David Kaye, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 2: Arun Chinmayi, Civil Society, Asia-Pacific Group
Speaker 3: MacKinnon Rebecca, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

How can a multistakeholder approach contribute to the development of both government and platform level regulations for online content?
What principles should be used to structure approaches to regulating content online?
How do we go about protecting free expression while also preventing the most serious negative impacts of online content?

Relevance to Theme: The goal of this panel is to help develop structures to ensure that approaches to improving online content take into account the perspectives of a range of stakeholders. As we think about moving towards a more secure, stable and resilient online space, developing multistakeholder approaches to these problems will be critically important.

Relevance to Internet Governance: The panel is focused on new approaches to the development of regulations at both the national government level, at the platform level, and in the development of principles at the global level. We hope that this new model will play an important role in internet governance in the future.

Format:
Round Table - Circle - 90 Min

Description: Social media and the internet have dramatically changed the way we exchange information. Digital spaces provide incredible opportunities, but also present brand new challenges that governments, tech companies and citizens are still struggling to effectively tackle. This roundtable will function as a workshopping exercise, to develop the practical terms of a participatory, multistakeholder approach to the moderation of online content. The need for a multistakeholder model to help address content online is grounded in the interplay between several increasingly troubling trends: first, governments are considering or passing legislation that pose very real threats to freedom of expression online; second, private sector companies exercise extraordinary control over what is and is not allowed on their platforms, which have increasingly come to represent a substantial proportion of the public square, with very little transparency or accountability in their processes; and third, the urgent need to combat harmful online content, while protecting and respecting core commitments to freedom of expression.

With input from speakers who are experts in online content and human rights, this roundtable will focus on answering practical questions about elements of a feasible multistakeholder model for a social media council. Some key questions will include: How should we properly structure such bodies to ensure effectiveness, buy-in from governments and platforms, and protection of foundational human rights principles? Who should be a member of such a body? How should members be selected? What will be the specific function of such a body: will it review individual appeals on content, or serve as an advisory body to help establish global standards? Should there be a single body, or should there be national- or regional-level bodies?

This event at IGF will build on input from previous meetings the co-sponsors have convened at Stanford University, at RightsCon in Tunis, and at World Press Freedom day in Addis Ababa. We expect that the roundtable will play an important role in the creating a new global multistakeholder body to tackled challenging governance issues related to challenging online content.

Expected Outcomes: This session will directly inform the process of consulting and designing a multistakeholder social media council for online content moderation. Participants will directly contribute to the development of these bodies through their input, and by helping to tackled outstanding practical questions. This will form the cornerstone for

Discussion Facilitation:

We hope that this will be a very participatory roundtable. We will begin the conversation by asking each of the speakers to briefly address some core questions, but very quickly will open the discussion to the audience. This discussion will be structured around core questions, developed in advance and designed to elicit participation, and to structure the conversation around getting input that will facilitate moving the idea forward practically.

Online Participation:

We hope that the online participation tool will allow us to get feedback from an even broader range of stakeholders than those in attendance at IGF. We hope that this tool will allow feedback on our core questions from those off-site and will contribute in useful ways to the conversations in the room.

SDGs:

GOAL 4: Quality Education
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

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

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):

Domain Name System
Human Rights
Illicit content

Organizer 1: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 3: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 4: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 5: Private Sector, Asia-Pacific Group
Organizer 6: Technical Community, Latin American and Caribbean Group (GRULAC)

Speaker 1: Bertrand de La Chapelle, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Polina Malaja, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Manal Ismail, Government, African Group
Speaker 4: Jennifer Chung, Technical Community, Asia-Pacific Group
Speaker 5: Susan Chalmers, Government, Western European and Others Group (WEOG)
Speaker 6: Thomas Rickert, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

Two policy questions will guide discussions throughout the session. The first one deals with the different layers that, combined, enable the Internet to work. The second one delves into the issue of responsibility.

- Policy question #1: Is “blocking access to illegal online content in the level of DNS infrastructure” as effective as “removing illegal content by taking action against the owner/publisher or the hosting providers”?

- Policy question #2: Should DNS operators play any role in general efforts aimed at tackling illegal content on the Internet? If DNS operators have any role to play, should they bear the same responsibilities as hosting providers and publishers of illegal content or should they have a different legal treatment? What are the risks inherent to a one-size-fits-all approach to the matter?

In the end, both questions require a risk assessment to allow for an evaluation of the direct and indirect implications of each possible response.

Relevance to Theme: The Domain Name System (DNS) is an addressing system upon which all networks that form the Internet rely. Its correct and neutral operation is fundamental to the security, stability and resilience of the Internet (and therefore of cyberspace as a whole). The Global Commission on the Stability of Cyberspace has recently described the DNS as one of the key parts of the “public core of Internet” (together with the Internet’s numbering system, packet routing and forwarding schemes, the underlying physical transmission media, as well as cryptographic mechanisms used for authentication and identity).

As Internet penetration and usage increase worldwide, more cases of user abusive behaviour and the publication of illicit content become visible and known to the general public (e.g.: hate speech, child sexual abuse material, terrorist content and propaganda, sales of counterfeit products, trademark and copyright violations, etc.). Increasingly, registries and registrars have been requested or forced (either through court orders or private notice & takedown requests that) to perform changes to the DNS space under their responsibility by cancelling, transferring, deleting or suspending domain names as a means to tackle illicit or abusive content available on the Internet. Sometimes, depending on the legal regime applied to intermediaries, registries and registrars run the risk of being held liable for third party content on the Internet.

While resorting to the DNS seems to be a rapid alternative to blocking access to abusive content or activities online, it does not provide an effective and sustainable way to remove content from the Internet, because new domain names might be easily be acquired for replacing those that become eventually

cancelled or suspended and the content itself remains available on running servers maintained by those who produce and publish it and/or hosting provider they use. More importantly, interventions at the level of DNS operation can endanger the availability, the correct operation and the usability of the Internet for three main reasons. First, one single domain name can refer to an array of different servers, other domains and even whole networks. A domain name is larger in scope than an individual URL that generally indicates in a narrow sense the specific illicit content. To target a domain name might generate disproportional consequences and do damage to a collection of legitimate content and activities online, rendering very significant portions of the Internet unavailable. Second, due to the transnational nature of the DNS, local interventions in the system based in locally applicable legal norms can have cross-border effects that generate legal uncertainty and unleash what some have called a "legal arms race" that further contributes to technical, economic and political instability surrounding the Internet ecosystem. Finally, the large number of actors demanding solutions for tackling illicit content online coupled with an even larger number of actors and entities involved with DNS operation have generated uncoordinated policy and regulatory responses (from voluntary codes of conduct to extrajudicial trusted notification schemes between private parties and between public authorities and private operators) that have further aggravated the problem.

Due to the decentralised nature of the Internet and the difficulties inherent to tackling illicit online content, several stakeholders have been exerting pressure (including by demanding policy and regulatory intervention) over DNS operators in order to curtail access to illicit activities and content at the level of the DNS (sometimes even with extraterritorial and jurisdictional implications). On that front, important work has already been carried out by the Internet & Jurisdiction Policy Network in the development of operational norms, criteria and mechanisms to guide the practice of all stakeholders vis-à-vis the DNS in cases that deal with technical abuse and illicit content. Building on that, the proposed workshop aims to promote an in-depth and focused analysis of the latter topic (illicit content) within the scope of the 2019 IGF, guided by a risk-based approach to raise awareness of the direct and indirect implications of indiscriminate action against the DNS (and in consequence affecting the security, stability and resilience of the Internet as a whole).

Relevance to Internet Governance: One of the biggest challenges on Internet Governance is striking a balance between freedom of expression and security, sometimes incorrectly portrayed as contradictory. That challenge is amplified by the fact that some of the inherent characteristics of the Internet (e.g. global reach, openness, permissionless innovation and generativity) allow for the production of an almost infinite amount of content both in terms of quantity and in terms of quality. Furthermore, tackling illicit online content is not a simple undertaken, due to the fact that what is illicit in one jurisdiction might not be illicit in others. And, most importantly, there is little consensus on the proper methods and tools for dealing with abusive materials made available online. Uncertainty that surrenders those aspects of the discussion have a clear cut relation to goals #9, #16 and #17 of the SDGs. Industry, innovation and infrastructure development depend on flexible yet stable normative frameworks to flourish. Strong and accountable public and private institutions which operate or act upon DNS infrastructure are fundamental to the achievement of social justice and peaceful coexistence. And solid, cooperative, collaborative, inclusive and democratic partnerships (in line with the tenets of multi-stakeholderism) are essential to further and achieve the previous goals (as well as all of the other goals altogether).

The development and adoption of appropriate measures to deal with the issue of abusive online content shall be conducted in a manner that is consistent with the characteristics of the Internet, protects intermediaries from unreasonable burden and is respectful of the rights of its users, something that has been widely recognized by the WSIS, mainly in the Tunis Agenda (e.g. paragraph 43), reinforced by the NETmundial Declaration in 2014 (as it reiterates human rights protections online and the unified and unfragmented characteristic of the global Internet) and furthered ever since by other processes and fora in the last five years (for instance, the OECD Principles for Internet Policy Making, the initial documents produced by the UN Secretary General's High-level Panel on Digital Cooperation, the UNESCO Roam Principles, the anti-abuse work being conducted within the ICANN community, which led to a solid reporting platform for abusive practices, among others).

The reduction, mitigation and combat against the proliferation of abusive content should not be dealt with unilaterally either by governments through legislation or the private sector through autoregulation and self-

regulation. Because those actions can affect freedom of expression and other fundamental human rights (e.g.: freedom of association and of assembly), civil society has a concrete role to play in any discussion of the matter. Moreover, people from the technical community are essential in such debate, especially those who work on a daily basis at the forefront of incident handling and activities focused on the security, stability and resilience of the Internet as a whole.

From a procedural standpoint, the collaborative dialogue among those stakeholder groups around the topic in question can yield better results if it follows some widely recognized principles that can ensure open, consensus driven, transparent and accountable, inclusive, equitable and participatory activities. With that spirit in mind, as the IGF is the main focal point for Internet policy discussion worldwide, this workshop intends to serve as a platform for the convergence of different initiatives that have been dealing with the topic and for mapping good and bad examples of local legal frameworks applicable to the DNS as well as of policies and initiatives adopted by DNS operators to deal with illegal online content.

Format:

Other - 90 Min

Format description: Town Hall model will be applied - auditorium or classroom

Description: Methodology & flow of session:

The session will apply an adapted version of the “Town Hall model” to enable both a controlled as well as a free style of multistakeholder dialogue and aim at providing an overarching conversation by a very plural group of participants on all of the aspects inherent to the topic under discussion. A local stakeholder has been invited to bridge global discussions to the current landscape of Germany.

It will be structured around a brief presentation of (a) the relevance of the topic, (b) its relation to Internet governance and the SDGs and (c) the policy questions selected for discussion by the onsite moderator (5min). Two brief interventions (10 minutes each) will kick start discussions: one will present a “global status” of the Internet and jurisdiction debate, with a special focus on activities that explored the DNS as an avenue to tackle illicit content and endangered the security, stability and resiliency of the Internet; the other one will present the European experience vis-à-vis the role of DNS operators in fighting illicit content online.

After that, the moderator will entertain open-ended discussions about the first and the second policy questions in sequence (30 minutes each). In each 30-minutes segment, the moderator will give the floor in a random fashion (seeking to keep a multi-stakeholder balanced) to people on site and people following the session remotely. The audience will be able to engage with comments and questions (2 minutes each) directed to the invited speakers/participants, who cover a wide array of stakeholder groups as described in the “co-organizers” and “speakers” sections below (ccTLD and gTLD operators, technical community organisations, companies, government officials). Comments and questions might also be directed to other people in the audience.

The last five minutes of the session will be used by the moderator to summarise discussions and point out further avenues for future dialogue.

Synoptic session agenda:

- Introductory remarks by the moderator - 5 minutes
- Short introduction on the “global status” of the Internet and jurisdiction debate - 10 minutes
- Short introduction on the European experience - 10 minutes
- Open-ended Q&A session among participants (two segments)
-- Policy question #1: Is “blocking access to illegal online content in the level of infrastructure” as effective as “removing illegal content by taking action against the owner/publisher or the hosting providers”?

-- Policy question #2: Should DNS operators play any role in general efforts aimed at tackling illegal content from the Internet? If they have any role to play, should DNS operators bear the same responsibilities as

hosting providers and publishers of illegal content or should they have a different legal treatment? What are the risks inherent to a one-size-fits-all approach to the matter?

- Concluding remarks by the moderator - 5 minutes

Expected Outcomes: - Outreach with multiple and distinct stakeholders in order to spread the word and include more people on the debate.
- Build new networks for discussion and collaboration on the topic.
- Detailed report: map of good and bad examples of local legal frameworks applicable to the DNS as well as of policies and initiatives adopted by DNS operators to deal with illegal online content.
- Potential impact on policy making through the diffusion of the workshop results.

Discussion Facilitation:

The discussion will be facilitated by the onsite moderator who will guide the debate in each of the proposed segments for the workshop. The online moderator will make sure the remote participants are represented in the debate. Online participation and interaction will rely on the WebEx platform. Those joining the session using WebEx (either invited members of the Town Hall or the general audience) will be granted the floor in the segments of the workshop. The person in charge of the moderation will strive to entertain onsite and remote participation indiscriminately. Social media (twitter and facebook) will also be employed by the online moderator who will be in charge of browsing social media using some hashtags (to be defined).

Online Participation:

Online participation and interaction will rely on the WebEx platform. Those joining the session using WebEx (either invited members of the Town Hall or the general audience) will be granted the floor in the segments of the workshop. People in charge of the moderation will strive to entertain onsite and remote participation indiscriminately.

Proposed Additional Tools: Social media (twitter and facebook) will also be employed by the online moderator who will be in charge of browsing social media using some hashtags (to be defined).

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #341 Roadmap for confidence building measures (CBM) in cyberspace

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
International Norms

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Western European and Others Group (WEOG)

Speaker 1: Kaja Ciglic, Private Sector, Eastern European Group
Speaker 2: Nikolas Ott, Intergovernmental Organization, Intergovernmental Organization
Speaker 3: Alissa Starzak, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Kerry-Ann Barrett, Intergovernmental Organization, Latin American and Caribbean Group (GRULAC)
Speaker 5: PABLO CASTRO, Government, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

What would characterize effective confidence building measures to develop trust and reduce tensions in cyberspace?
How should confidence building measures in cyberspace mirror those used in conventional domains of conflict and in what ways should they differ?
What role can other stakeholder groups play in helping states both develop and implement confidence building measures for cyberspace?

Relevance to Theme: Amidst the current atmosphere of escalating tensions between nations in cyberspace, resulting in the development of increasingly sophisticated cyberweapons, it is more important than ever that nations pursue effective confidence building measures (CMBs) to establish trust and promote greater stability online. The economic and social benefits brought by increased connectivity are at risk in the face of an arms race between competing nation states that threatens to envelop innocent users, critical infrastructure and other private entities as collateral damage.
CBMs for cyberspace may reflect similar efforts to promote stability in traditional domains of conflict – air, land, sea and space – but will also need to take into account the unique challenges of building trust in a non-physical domain where attacks and capabilities are hidden. To inform this discussion, the session's panel will draw on the experiences of those with a diversity of perspectives and multidisciplinary backgrounds in cybersecurity technology and policy, as well as those with backgrounds in other areas of statecraft, to explore how different stakeholder groups can cooperate to help implement CBMs that support stability in the online ecosystem.

Relevance to Internet Governance: The challenge addressed in this proposed session is how to proactively and intentionally coordinate actions to create systems and structures that build trust between nations and reduce suspicions and tensions in cyberspace, leading to a meaningful reduction in the number and severity of threats online. This discussion cuts to the core of a number of internet governance challenges and inherently requires engagement by a range of stakeholders to explore how such confidence building measures should be designed and implemented – based on established norms and expectations – to protect a safe and secure internet.

Format:
Panel - Auditorium - 90 Min

Description: This session will take an expansive look at confidence building measures (CBMs) in cyberspace. An accelerating arms race between nations in the "fifth domain of conflict" – cyberspace – is likely to continue unabated without the imposition of meaningful processes and dialogues meant to reduce tensions and promote trust among competing and even allied countries. Such activities can mirror traditional approaches to confidence building in other conflict domains, including diplomatic engagements, information sharing, and technology exchanges, but might also involve innovative new approaches unique to cyberspace – including focusing on cooperative cybersecurity capacity building.
The development of confidence building measures for cyberspace will need to leverage a diversity of perspectives, including those who have a knowledge of the technology and challenges posed by cybersecurity, as well as those who understand the nuances of statecraft that make such CBMs effective in other domains of conflict and interstate competition. To this end the panel will gather speakers to represent government perspectives and those of intergovernmental organizations, as well as speakers to share insights from civil society, academia and the technology industry.
The session format will allow speakers to present their respective points of view as it relates to the potential

of CBMs in cyberspace, as well as the opportunity to challenge and respond to one another on which approaches might be most effective. Importantly, the session will help educate those attending the session on this emerging area of cyber diplomacy and leave ample time for questions directly from those in attendance to the panelists.

Agenda:
• 5 minutes – Opening remarks from moderator setting the stage for the discussion, highlighting the current state of affairs as it relates to the pursuit of confidence building measures between states in cyberspace and letting those attending the panel know that a substantial amount of time will be saved for questions in the later portion of the session.
• 25 minutes – Opening remarks from panelists sharing their perspectives on the major opportunities and challenges in establishing effective confidence building measures in cyberspace, and the ability of various stakeholder groups to support or hinder these efforts.
• 30 minutes – Moderator asks pointed questions to respective speakers about avenues for advancement in this space and highlighting where there seem to be obstacles to further progress. Speakers will respond both to direct questions as well as to one another, representing both their individual and stakeholder perspectives as it relates to the positions of others. This portion of the session will identify points of agreement and divergence for those in attendance.
• 30 minutes – Those attending the session, in the room or remotely, will be welcomed to ask direct questions of the speakers and share differing perspectives related to the development of confidence building measures in cyberspace. Once again, speakers will be encouraged to both address the questions that are asked as well as to respond to the answers provided by their colleagues.

Expected Outcomes: This session will provide important learnings and highlight significant opportunities for those in attendance from all stakeholder groups seeking to find ways to improve the cybersecurity ecosystem through meaningful actions to promote trust and increase capacity among states in cyberspace.
For representatives from nations still establishing a posture on these issues, this session will highlight the various forums and opportunities for multilateral, regional and bilateral engagements pursued by other nations to advance their interests and build relationships in this space.
For countries that have already been active in cyber diplomacy in recent years, this dialogue will provide an opportunity for them to share their insights and learn from others about what could be innovative new approaches to building trust and establishing cooperative relationships with governments and other stakeholders to reduce tensions and increase security online.
For representatives from other stakeholder groups, including industry and civil society, the panel discussion will serve to illuminate the current status of an emerging and critically important policy space, as well as highlight the ways in which other stakeholders can contribute to government efforts at cyber diplomacy.

Discussion Facilitation:

The moderators will work to ensure that the discussion at the outset of the session highlights the current state of play in the issue space and then prompt speakers to actively engage with and respond to one another. Moderators will also keep the timing of the discussion on track to allow for a half hour of audience questions at the end of the session, which they will make attendees aware of at the outset to promote thoughtful questions and comments in response to speakers. The onsite and online moderators will work together to make sure audience questions are taken from a diverse collection of session attendees, both on site and online.

Online Participation:

The online moderator will manage remote participation in the session via the Official Online Participation Platform, ensuring that those who are virtually attending the panel discussion are able to view/listen throughout its entirety, and that they are actively included in the question and comments portion from session attendees.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #344 Meaningful election participation in a time of social media

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Civic Engagement online
Fake News
FoE online

Organizer 1: Civil Society, Asia-Pacific Group

Speaker 1: Nighat Dad, Civil Society, Asia-Pacific Group
Speaker 2: raymond Serrato, Intergovernmental Organization, Western European and Others Group (WEOG)
Speaker 3: Ankhi Das, Private Sector, Asia-Pacific Group

Policy Question(s):

1. What role should social media companies have in election online campaigning?
2. How can online political conversations be made more accessible?
3. How much internet regulation should governments engage in to ensue free and fair elections?

Relevance to Theme: Political participation and elections with reference to the internet are now increasingly tied to questions of content, misinformation, online violence, safety and freedom of expression. These intersecting issues have been put to the test in the response of social media companies, governments, political parties and citizens with regards to the internet.

Relevance to Internet Governance: Political participation is integral to the exercise of human rights online--it is intimately tied to concepts of free speech, association and assembly in online spaces. The opening up of online spaces as sites of political discourse also opens up questions of regulatory and legal frameworks that speak to questions of policy that are central to the multi-stakeholder framework of the IGF. While political participation is a now accepted concept of digital spaces, the emerging issues to be tackled in this panel speak directly to the evolving nature of the political and the human rights implications that inhere.

Social media, once greeted with wide-eyed enthusiasm and uncritical embrace as tool for political participation has now come to shake the very foundations of modern democracies. The glare of the media and regulators has been on the Brexit and Trump campaigns for the proliferation of misinformation and political manipulation. These trends have been observed all over the world, however the dynamics have varied in different contexts. This panel aims to highlight the different trends in electoral and political participation from around the world.
The role of technology in effecting and manipulating political outcomes needs to be contextualized and seen through the lens of regional trends. The way technology is employed for electioneering is not uniform—WhatsApp, for instance, emerged as one of the primary sources for misinformation and propaganda in the Brazilian elections, however it did not feature heavily in the United States elections. Political participation on social media is also stymied by political and gendered abuse and harassment. The experience of women is often seen as less as a political concern and more of a person affront—however it has real political implications for the participation of female candidates and voters. Access, or lack thereof, is an impediment

to participation in online political discourse. Now that a lot of political conversations are taking place online, those without access experience a political exclusion that is to become even more acute.

Format:

Debate - Auditorium - 90 Min

Description: This session will seek to unpack the question of political participation and the role of technology in ensuring political access for different genders, classes and religious/racial minorities within political discourse and electoral participation. The promise of the internet has been that it has democratised political participation through greater access to information and shifting political conversations to the participatory mediums such as social media. This optimism has been tempered by the hierarchical structuring of the internet in terms of its uneven access to ICTs, political censorship, network shutdowns, misinformation as well as hate speech and harassment online.
This session will also seek to go beyond this straightforward analysis by bringing in stories and lived experiences of online political commentators from different countries, both the Global South and North, as well as speaking to gendered and racial experiences in terms of politicising personal narratives through digital platforms. We seek to deconstruct the nature of the "political" in online spaces and define it within the experience of our panel participants.

Expected Outcomes: 1. Awareness raising: presentation of research on elections and social media from around the world;
2. Drawing meaningful comparisons from across the world and potential for combined research;
3. Suggestions and recommendations for social media companies, governments and policy-makers.

Discussion Facilitation:

The initial arguments for the debate will be set out by the selected speakers, however after half an hour the debate will be opened to the audience. Speakers will be given the chance to rebut some of the comments from the audience but the focus will be on the audience during this part.
Efforts will be make to ensure that organisations in Germany and others working on political participation are represented in the audience through invitations and online promotions leading up to the event.

Online Participation:

The moderator will be collecting questions coming in from online participants and posing them to the speakers in the last 10 minutes.
Furthermore, different activists--especially from the Global South--from different countries will be asked promote the online participation tool so that a diverse set of participants tune into the event remotely. This is important since countries such as Germany are inaccessible for several countries for reasons of finance and stringent visa policies.

SDGs:

GOAL 5: Gender Equality
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #345 Resilient Digital Democracy: the role of internet standards

Theme:

Security, Safety, Stability and Resilience

Subtheme(s):

Human Rights
Internet Protocols
Resilience

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, Eastern European Group
Organizer 3: ,
Organizer 4: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Tara Whalen, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Ndeye Maimouna DIOP, Civil Society, African Group
Speaker 3: Benoit Ampeau, Technical Community, Western European and Others Group (WEOG)
Speaker 4: Raquel Gatto, Technical Community, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

The overarching question discussed by the panel will be: How can techno-policy standards, among others in the field of data privacy and data protection, participate in supporting the resilience of the rule of law and human rights in a democratic and inclusive digital societies?

The policy questions which will be addressed are:
- Human rights
- Data privacy & protection
- Internet protocols
- The collaboration of different stakeholders to create resilient standards

Relevance to Theme: Resilience is the capacity of a system react to an attack and recover. Achieving resilience in communication systems was the one of main drives behind the invention of distributed systems. The Internet is now a key infrastructure, driving growth and innovation worldwide. People and businesses rely on it to communicate, share ideas, and do business. However, the Internet has been fertile ground for new cyberthreats. Pervasive monitoring has been recognised as a threat by the technical community in RFC 7258. Recent research in Security Studies by Raab et al. (2015, 2018) has shown that privacy and data protection properties of social systems are key elements in achieving the societal resilience of democratic values and fundamental rights, such as freedom of expression and freedom from unfair discrimination. Other leading-edge research (see: Doty and Mulligan, 2013) has shown the role played by some Internet standards in ensuring privacy and data protection properties are embedded into Internet protocols and infrastructure. Finally, other branches of research have shown that architectural choices in the design of Internet infrastructure affect privacy and data protection properties of the system, and thus the capacity of affected societies to develop resilient democratic structures (Musiani, Cogburn, DeNardis and Levinson, 2016).

This panel would like to facilitate dialogue between stakeholders and across communities in Internet governance to further our common understanding of the relation between democracy, resilience, privacy and data protection as resilience-enabling properties of digital infrastructure, and the development of techno-policy standards.

Relevance to Internet Governance: By launching a discussion between stakeholders from different communities, geographic areas and cultures, this session would like to explore how to better integrate goals of democratic and human rights resilience in the development of Internet standards affecting properties of the infrastructure, such as data privacy and protection, that are enablers of such resilience. A set of best practices is a desired outcome of this session.

Format:
Round Table - Circle - 90 Min

Description: Techno-policy standards play a key role in supporting a resilient democratic digital society. Privacy and Data Protection by Design approaches can be transposed into Human Rights by Design approaches, and implemented into the infrastructure through Internet standards. This panel will explore the potential of such standards.

AGENDA

=> Surveillance, Resilience and Privacy in Democratic Societies
The chair and moderator will open the discussion by giving an introduction to recent research results and policy solutions in their fields of expertise.

=> Data Protection and Democratic Resilience : How data protection and privacy protection contributes to the strengthening of democratic values and fundamental rights.

=> Web/Internet Standards, Resilience and Human Rights

=> Human Rights Considerations in Web Protocols: what methodology could be implemented? How human rights and democratic values can be turned into properties of a communication system. This talk will reflect on recent work on human rights in IRTF HRCIP and W3C PING.

=> Infrastructure, Democratic Resilience and Free Speech
In this talk, a leading expert will give a report on changes that can be observed in communication infrastructure in war-torn regions, and how Privacy Enhancing Technologies, especially once embedded into digital infrastructure, can help affected users and communities adopt resilient behaviours to protect their fundamental rights, especially their right to free speech and access to information.

=> Q&A and debate moderated by the chair and the online moderator (40 min)

Expected Outcomes: The workshop aim at producing concrete suggestion on how Internet protocols can preserve the resiliency of democracy.

As such, following an in-depth policy discussion between high-level stakeholders coming from different backgrounds, and taking into account discussions with the audience, rapporteurs will draw from these discussions to propose a number of ideas and best practices that can be implemented in internet governance fora in order to further the efficiency of mechanisms ensuring Internet protocols are developed in a way that preserves the resilient capacities of democracy and human rights in digital societies.

Discussion Facilitation:

Preparation calls: Several preparation calls will be organized in advance of the workshop to enhance interaction and share views. A session dedicated to privacy standards in the European context will also be organized during the French Internet Governance Forum foreseen on July 4th. The present session aim to broaden the discussion to implement a global approach.

Moderation and online tools: The chair and moderator are policy experts and well versed in animating multistakeholder discussions at the global level. Question will be prepared in advance to engage both the audience and speakers to think out of the box.

We also aim at engaging the audience by enabling them to contribute directly to the workshop. We plan to use complementary tools in order to allow participants to vote in real time (mobile polling app and website directly accessible in the participant browser) on questions addressed to the panelist. The online moderator will manage a Q&A tool to allow direct interaction with audience remotely.

The workshop will be promoted in advance through social media networks and various online media platforms, including the organizers' own websites.

Online Participation:

The remote moderator will be involved throughout the session to enhance remote participation. Both chair and moderator will ensure views and reactions of remote participants are reflected in the discussion. The remote moderator will also attend IGF training sessions.

Remote participants will also be given the opportunity to participate, on equal footing, to online polling (mobile polling app and Q&A questions).

Proposed Additional Tools: We plan to use complementary tools in order to allow participants to vote in real time in particular the mobile polling app Mentimeter.

We also plan to use social media platforms to promote the workshop in particular remote participation and create awareness.

A number of documents will also be shared online (draft RFC, academic literature and ressources)

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #348 Can cyberweapons be developed and used responsibly?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Eastern European Group

Speaker 1: Jan Neutze, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Suzanne Spaulding Suzanne Spaulding, Government, Western European and Others Group (WEOG)
Speaker 3: Camille François, Private Sector, Western European and Others Group (WEOG)
Speaker 4: Abdul-Hakeem Ajijola , Private Sector, African Group

Policy Question(s):

Recognizing that States have a responsibility to national security and defense, is there a way for governments to responsibly pursue military capabilities in cyberspace that doesn't threaten to unnecessarily jeopardize innocent civilians and other parties?
What would characterize a responsible military presence in cyberspace as opposed to irresponsible pursuits?
What role can other stakeholders, including industry and civil society organizations, play in identifying responsible behavior as it relates to military cyber capabilities and holding states accountable to such behavior?

Relevance to Theme: This session will directly address concerns at the core of the "Security, Safety, Stability and Resilience" theme of the IGF by exploring how governments can uphold their national security responsibilities while not jeopardizing the security of individuals and the broader online ecosystem. At a time when nation states are playing an ever-larger role in the development and use of cyberweapons, which can be easily misused or repurposed for malicious ends, it is critical to explore what processes and procedures can be put in place to limit the dangers posed by these advanced capabilities in partnership with other governments and stakeholders to preserve a safe and secure online world.

Relevance to Internet Governance: This session addresses the core of internet governance as it seeks to further develop norms and expectations to limit the frequency and sophistication of threats online by leveraging multistakeholder perspectives to identify the characteristics of responsible state actions in the development, maintenance and implementation of military capabilities in cyberspace. This will include highlighting the rules and decision making processes which should govern activities in this space.

Format:

Panel - Auditorium - 90 Min

Description: Can cyberweapons be developed and used responsibly?
Amidst escalating numbers of sophisticated cyberattacks – many of which are conducted on behalf of governments or leverage tools developed by government actors – this session will explore whether or not there is a responsible way for states to develop, maintain and employ military cyber capabilities in the interests of national security and under a right to self-defense. Among other things, this session will touch on subjects including vulnerability disclosure, government transparency, kinetic versus cyber-attacks, and nation-state responsibility in the event of a misused or stolen cyberweapon.
Each year, increasing numbers of governments decide to invest considerable resources in establishing military capabilities in cyberspace. This decision is often made with little input from citizens or outside groups and the activities of the resulting "cyber units" are generally shrouded in secrecy. This panel will provide an important opportunity for feedback and input on these activities from a diversity of stakeholder groups to promote responsible behavior that prioritizes the security of the entire online ecosystem.
The session format will allow speakers from industry, academia and civil society groups to share their thoughts on what would characterize responsible behavior by governments as they seek to achieve national security objectives in cyberspace. In addition, the session will also give those with experience in government the opportunity to provide greater context and insight into government decision making related to the militarization of cyberspace. The discussion will hope to provide valuable learnings to those in attendance seeking to influence or guide government activities in this space and provide ample time for questions for the speakers.

Agenda:
• 5 minutes – Opening remarks from moderator setting the stage for the discussion, highlighting the current state of affairs as it relates to the militarization of cyberspace and the pursuit of offensive capabilities by governments, and letting those attending the panel know that a substantial amount of time will be saved for questions in the later portion of the session.
• 25 minutes – Opening remarks from panelists sharing their perspectives on what, if any, are examples of responsible military postures in cyberspace and what constitutes irresponsible behavior.
• 30 minutes – Moderator asks pointed questions to respective speakers about what best practices should be adopted to minimize the unintended dangers posed by military cyber operations. Speakers will respond both to direct questions as well as to one another, representing both their individual and stakeholder perspectives as it relates to the positions of others. This portion of the session will identify points of agreement and divergence for those in attendance.
• 30 minutes – Those attending the session, in the room or remotely, will be welcomed to ask direct questions of the speakers and share differing perspectives related to the development of offensive capabilities in cyberspace. Once again, speakers will be encouraged to both address the questions that are asked as well as to respond to the answers provided by their colleagues.

Expected Outcomes: This session will provide important learnings and highlight significant opportunities for those in attendance from all stakeholder groups seeking to find ways to improve the cybersecurity ecosystem by promoting responsible behavior on the part of states in pursuit of national security objectives online.

For government representatives, the session will highlight best practices and innovative new approaches to the development of military capabilities in cyberspace - including on issues like transparency and vulnerability disclosure. Meanwhile, other stakeholders from industry and civil society will have an opportunity to learn about ways to continue influencing this discussion in favor of solutions that protect the entire online ecosystem.

Discussion Facilitation:

The moderators will work to ensure that the discussion at the outset of the session highlights the current state of play in the issue space and then prompt speakers to actively engage with and respond to one another. Moderators will also keep the timing of the discussion on track to allow for a full half hour of audience questions and comments at the end of the session, which the moderators will make attendees aware of at the outset to promote thoughtful questions and comments in response to speakers. The onsite and online moderators will work together to make sure audience questions are taken from a diverse collection of session attendees, both on site and online.

Online Participation:

The online moderator will manage remote participation in the session via the Official Online Participation Platform, ensuring that those who are virtually attending the panel discussion are able to view/listen throughout its entirety, and that they are actively included in the question and comments portion from session attendees.

SDGs:

GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #354 Capacity building of children for improved mental health

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Child Online Safety
Cyber Security Best Practice

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, Asia-Pacific Group

Speaker 1: Nighat Dad, Civil Society, Asia-Pacific Group
Speaker 2: Shmyla Khan, Civil Society, Asia-Pacific Group
Speaker 3: Smita Vanniyar, Civil Society, Asia-Pacific Group

Policy Question(s):

How can children's rights to participation, access to information, and freedom of speech be preserved and balanced with their right to be protected from violence, exploitation and sexual abuse in the online environment?
How can their resilience be increased by means of capacity building, media literacy, support and guidance in the digital environment?
What strategies are being used in other countries to protect children from online abuse and violence that can be duplicated in Pakistan?

Relevance to Theme: The proposed session aims to chalk out ways to build capacity and resilience in children and youth to protect them from violence, exploitation and sexual abuse rampant in online spaces.

Relevance to Internet Governance: The session proposes to ensure that the needs of children and youth as consumers of the internet are respected and addressed in order to protect them from online abuse and violence.

Format:
Round Table - Circle - 90 Min

Description: Children and youth all over the world are more susceptible to online abuse, though it may range and vary in shape or form, the gist of it remains the same and along with the offline threat they are also trolled and bullied online. This brings with it a base level of resistance and isolation that only builds with the shift in the cultural landscape.
The session is aimed at discussing and highlighting the causes, reactions, and the toll on the mental and physical health of children and youth precipitated by online abuse. The session will discuss the idiosyncratic ways in which children deal with abuse and strategies that can be adopted to build their resilience. The sessions will also explore ways in which we can protect children and youth from falling prey to online bullying. Children and young adults face online bullying across the world but it's important to understand how they deal with it and how they can come together and deal with these problems and learn from each other to build resilience
It will be in the form of a round table discussion and attendees will share how they are working in their respective countries to combat this problem. Attendees will interact and learn from each other succeeded by a compilation of strategies that can be adopted to address this problem.

Expected Outcomes: List of strategies and ways to combat online abuse in a particular age group, that are already in practice in other countries.

Discussion Facilitation:

This session will involve a 15-minute presentation with speakers presenting the issue and emerging risks of online child abuse and violence followed by a 75-minute discussion with attendees to list down strategies and ways to build the capacity of children to combat online violence and be more resilient

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 3: Good Health and Well-Being

IGF 2019 WS #355 IoT Security Awareness: Learning from the Youth

Theme:
Security, Safety, Stability and Resilience

Subtheme(s): Cyber Attacks
Cyber Security Best Practice
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, African Group
Organizer 3: Civil Society, Western European and Others Group (WEOG)
Organizer 4: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 5: Technical Community, Asia-Pacific Group
Organizer 6: Civil Society, African Group
Organizer 7: Civil Society, African Group
Organizer 8: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 9: Technical Community, African Group

Speaker 1: Ethan Sweet, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Lisa nyamadzawo, Civil Society, African Group
Speaker 3: Ihita Gangavarapu, Technical Community, Asia-Pacific Group
Speaker 4: Daniel Bill Opio, Civil Society, African Group
Speaker 5: Yawri Carr Quirós , Civil Society, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

IoT in Homes, Cars, Schools and Offices: What are the implications of IoT in modern society? How do we create better awareness about general best practices and potential security challenges regarding this technology? Is it possible to build more trust in these devices despite concerns about how interconnected they are becoming? Can collaboration between stakeholders help enact policies that help foster IoT security?

Relevance to Theme: Our intentions are to have comprehensive discussion about security issues in IoT and how we can avoid or circumvent them, but we will try to do this at the surface and not intentionally get too technical, keeping it simple. We will encroach on aspects that also proffer solutions to the security challenges in this domain. We will be reaching into areas regarding trust using IoT devices and possible short falls.

Relevance to Internet Governance: Our session intersects with Internet Governance because internet users (especially people that use internet enabled items) need to be in a safe environment and to feel safe most importantly; from security threats, hacks and data breaches (data theft). So we would like better policy programmes on IoT security by championing its awareness.

Privacy and human rights is the other matter because with IoT devices what confirms its true safety, regarding the data we share (data usage). The understanding needs to be open in terms of access and trust.

Format:
Birds of a Feather - Classroom - 60 Min

Description: Opting for a less than formal session with a bird of a feather classroom format, we do not primarily intend to work with agendas per say. Although we would all (organizers) be working with an objective for generating awareness and fostering inclusion on the topic. Session outline is likely to be as follows:

Before the workshop
5 minutes: Set up white boards and other preparations

At the workshop
5 - 7 minutes: Introductions: outline of general purpose and role of the session
Provide context to address relevancy

30 - 35 minutes: [Deep dive] Brainstorming on relevant IoT issues - like awareness, best practices, security cases, potential risks, solutions and the future of policy making etc (as we would like for an open authentic dialogue) - by forming small discussions groups, effectively breaking into mini groups (four to five or more) depending on our size, strategically positioning organizers that help facilitate discussions in each group and giving each person a chance to contribute specifically to the matter, each organizer being as dynamic and effective as possible to include everyone in the discussion.
Formulate strategic options in terms of solutions and best practices
Evaluate strategic options
What to prioritize and then idea reduction done to utmost relevancy

10 -15 minutes: Conclusion, summary and next steps
Building a movement in a coalition, grassroots education and activities to be considered.

Our open nature of the session would facilitate engagement and foster inclusion, we will as group inquire, include and consider ideas from everyone making sure we try to reach complete participation. In in-dept and inclusive dialogues about these issues we will draw more attention to them, facilitating awareness. Also since we would be looking out for best practices and solutions, this would be an avenue for educative and informative purposes.

Expected Outcomes: Achieved comprehensive and inclusive discussions about on IoT and its related issues
Fostered representation and inclusion regarding the matter
Increased awareness of present and future implications of IoT
Recommendations from the attendees on how to consolidate on IoT issues especially on security with proffered solutions

Discussion Facilitation:

Opting for a less than formal session with a bird of a feather classroom format, we do not primarily intend to work with agendas per say. Although we would all (organizers) be working with an objective for generating awareness and fostering inclusion on the topic. Session outline is likely to be as follows:

Before the workshop
5 minutes: Set up white boards and other preparations

At the workshop
5 - 7 minutes: Introductions: outline of general purpose and role of the session
Provide context to address relevancy
30 - 35 minutes: [Deep dive] Brainstorming on relevant IoT issues - like awareness, best practices, security cases, potential risks, solutions and the future of policy making etc (as we would like for an open authentic dialogue) - by forming small discussions groups, effectively breaking into mini groups (four to five or more) depending on our size, strategically positioning organizers that help facilitate discussions in each group and giving each person a chance to contribute specifically to the matter, each organizer being as dynamic and effective as possible to include everyone in the discussion.
Formulate strategic options in terms of solutions and best practices
Evaluate strategic options
What to prioritize and then idea reduction done to utmost relevancy

10 -15 minutes: Conclusion, summary and next steps
Building a movement in a coalition, grassroots education and activities to be considered.

Our open nature of the session would facilitate engagement and foster inclusion, we will as group inquire, include and consider ideas from everyone making sure we try to reach complete participation. In in-dept and inclusive dialogues about these issues we will draw more attention to them, facilitating awareness. Also since we would be looking out for best practices and solutions, this would be an avenue for educative and informative purposes.

Online Participation:

Using moderation, through cues and first-to-demonstrate the need to speak, we will be looking to foster participation online as well by switching between onsite and online participation, collaborating with the online moderator towards full inclusion.

Proposed Additional Tools: As a second option or fail safe we could opt to use the unofficial zoom platform for remote participation.

White board, cardboard papers, markers

We will wish to use the white boards for general or relevant group ideas or focus points and to pass general group information which would also serve as a reference and reminder.

Cardboard papers would be used for each individual group points and for helping preserve fresh ideas etc

Markers will be for writing on both the cardboard papers and the whiteboard

SDGs:

GOAL 9: Industry, Innovation and Infrastructure

Reference Document

IGF 2019 WS #356 Data security of end-users in the era of AI for SDG

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Capacity Building
Cyber Attacks
Trust and Accountability

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, African Group

Speaker 1: Dawit Bekele, Technical Community, African Group
Speaker 2: Olga Cavalli, Government, Latin American and Caribbean Group (GRULAC)
Speaker 3: Walid Al-Saqaf, Technical Community, Western European and Others Group (WEOG)

Policy Question(s):

How can consumer's data must be protect ?
What are the news Strategies and tools to protects end-users data on the AI World ?

Relevance to Theme: The mains of that Workshop is to learn more how and what are strategies, a new approach and powerful new tools to protect end-users data on the new world of AI to better achieve the SDG Goals more interactive with participants .

End-users's data security has become one of the top priorities for many multistakholer in the digital era. No one is immune to cyber threats. Over the years, the world has seen a dramatic increase in online attacks. Not only are these threats increasing in number, but they are also getting more sophisticated.
And we add to that the Artificial Intelligence, as you know Artificial intelligence (AI) is an area of computer science that emphasizes the creation of intelligent machines that work and react like humans.

We explore some Risks Everyone (End-Users) Should Know About for more data protection and risk of Hacking algorithms: It is now possible to track and analyze an individual's every move online as well as

when they are going about their daily business. Cameras are nearly everywhere, and facial recognition algorithms know who you are.

Relevance to Internet Governance: protect users data on connected world of Artifical Intellegence

Format:
Debate - Classroom - 90 Min

Description: We explore some Risks Everyone (End-Users) Should Know About for more data protection and risk of Hacking algorithms: It is now possible to track and analyze an individual's every move online as well as when they are going about their daily business. Cameras are nearly everywhere, and facial recognition algorithms know who you are.

Expected Outcomes: -People aware about their data
- They can organize local engagament and outreach
-People undertood Artifical intelligence (AI)
- people aware how to have better Connected World to Achieve the SDG Goald
-GDPR and aother Data protectiong Undertood

Discussion Facilitation:

1. 1st session of speakers, to present their view points (30min);
2. Interaction session with participants (onsite or online) (25 min);
3. 2nd session of the speakers, to bring more clarifications and to answer the questions (30 min) ;
4. Conclusions by the moderator (5min);

Online Participation:

Yes the remote Moderator can Take online Interaction /Question using Webex Official

SDGs:

GOAL 4: Quality Education
GOAL 9: Industry, Innovation and Infrastructure
GOAL 17: Partnerships for the Goals

IGF 2019 WS #359 Network disruptions across borders: a new cyber response

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Internet kill switch
Jurisdiction

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Civil Society, African Group

Speaker 1: Lise Fuhr, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Berhan Taye Gemeda , Civil Society, African Group
Speaker 3: Anriette Esterhuysen, Civil Society, African Group

Policy Question(s):

Is a network disruption ever a justifiable countermeasure or response to a cyber attack or operation? If so, what are the rules, norms, or laws—existing or aspirational—that govern the extent of the disruption? Given the wide impacts of such disruptions, who should take part in the development of these norms and laws, and in which fora?

Relevance to Theme: From a broad perspective, a nation's ability to reliably and consistently access the global internet is fundamental to its creation of a digital healthy, resilient, stable, and secure digital environment. Critical infrastructure depends on internet access to track and identify threats, while individual users are growing more reliant on internet-connected applications for their daily economic, social, and cultural activity, from accessing medical services to transacting business to remaining in touch with family. For these reasons, the decision by a foreign actor to actively disrupt a nation's access to the global internet is integrally important to security and safety, online and offline.

Relevance to Internet Governance: The capability of a state actor to prevent another state or population's access to the internet has the potential to broadly impact all stakeholder groups through a swift, decisive, and unilateral act. Given that this sort of powerful act has already taken place, the timeliness of this discussion is established. We propose to study the norms around cross-border disruptions from a variety of stakeholder lenses, attempting to broaden what has so far been a limited discussion of narrow, military interests and arcane legal rules. Few other measures command such fascination as kill switches, and we expect robust discussion of possible norms, procedures, and accountability structures to reign in this function as it begins to be deployed across borders. Governance of the internet by default involves cross-border considerations, and this topic -- despite its origin in more military or cyber scenarios -- squarely falls within the remit of existing internet governance institutions whose purpose is to protect and promote the shared evolution and use of the internet.

Format:

Round Table - Circle - 60 Min

Description: On November 6, 2018, the United States Cyber Command conducted an operation to silence the Internet Research Agency (IRA), the Russian "troll farm" that played an instrumental role in spreading mis- and dis-information ahead of the 2016 U.S. presidential election. The operation, which was conducted in an effort to "prevent the Russians from mounting a disinformation campaign" that would "cast doubt on the results" of the 2018 U.S. midterm elections, knocked the IRA offline temporarily. In the wake of the operation becoming public, a standing U.S. senator and an Obama-era National Security Council cyber advisor raised the question of whether the response was strong enough. If the U.S. government really wants to send a message, they said, they should disconnect the entire country from the internet. The Cyber Command operation and subsequent statements from officials raise an important question: to what extent are network disruptions a justifiable response to a cyber attack?

Network disruptions, or blackouts, are events where some or all internet end users' connections to the internet are disrupted. Network disruptions can be intentional or unintentional, and their effects are manifold. When access to applications like social media, mobile money, and messaging are disrupted, users are suddenly left without crucial information and links to family, friends, and institutions within and outside their countries. The many harms from such disruptions are beginning to be catalogued by civil society, as through the #KeepItOn Coalition against internet shutdowns, in conjunction with media.

To date, network shutdowns have largely been perpetrated by governments in order to limit their polity's access to the internet. However, more recently governments have taken to leveraging cyber capabilities to limit other countries' citizens' access to the internet. This roundtable workshop will discuss important questions implicated by this new trend, including:

● To what extent do existing internet and non-internet governance regimes (norms, laws, or standards) already provide guidance for the acceptability of this type of behavior?

● To what extent should network shutdowns be an acceptable countermeasure in response to a cyber attack? What sorts of limitations should be placed on state use of offensive cyber capabilities to disrupt network access?

● What are the implications (political, architectural, economic, human rights, and others) of the use of network disruptions in response to cyber attacks or campaigns?

The workshop will feature two 10-minute opening presentations from featured speakers, including the Director-General of ETNO and the leader of a civil society coalition against internet shutdowns. An academic will then moderate a roundtable-style discussion. The goal of the discussion is to gather a wide array of stakeholder perspectives in order to inform a more substantive policy discussion that expands the current discussion's aperture wider than the narrow, military focus currently embroiling it. Lessons and learnings would then be captured and published in a public outcomes document.

Expected Outcomes: ● Clearer understanding of:
○ The rules, norms, and laws governing the state use of offensive cyber capabilities to disrupt network access in countries other than their own.
○ The tradeoffs and implications of shutting down network access in another country, including the potential economic, social, political, architectural, and human rights implications.
○ The stakeholders in cyber policymaking and critical infrastructure management, with focus on those with authority over telecommunications networks.
● identification of the leverage points and advocacy pathways to increase inclusion and representation of viewpoints and equities beyond narrow military and legal considerations in cyber policymaking
● Published outcomes document to capture key lessons and learnings for presentation to policy- and decision-makers

Discussion Facilitation:

Speakers will come from vastly different perspectives, including the Director-General of the private sector telecom association ETNO, the leader of the #KeepItOn civil society coalition against internet shutdowns, and the public sector. The workshop will feature two 10-minute opening presentations from featured speakers, who will then moderate a roundtable-style discussion. The goal of the discussion is to gather a wide array of stakeholder perspectives in order to inform a more substantive policy discussion that expands the current discussion's aperture wider than the narrow, military focus currently embroiling it. We will present a lively cross-examination of their arguments. Lessons and learnings would then be captured and published in a public outcomes document.

Online Participation:

Before the event, we will advertise the workshop online through the robust social media channels of Access Now and the New America Foundation. We will elicit questions and comments before the event, and the online moderator will curate a presentation of these online contributions throughout the session, rather than waiting until the end as many sessions do.

SDGs:

GOAL 9: Industry, Innovation and Infrastructure
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

Reference Document

IGF 2019 WS #369 Questioning Parents and Society Responsibility on COP

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):

Capacity Building
Child Online Safety
Internet ethics

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, Asia-Pacific Group

Speaker 1: David NG, Civil Society, Asia-Pacific Group
Speaker 2: John Carr, Civil Society, Western European and Others Group (WEOG)
Speaker 3: ICT Watch Indonesia, Civil Society, Asia-Pacific Group
Speaker 4: Janice Richardson, Intergovernmental Organization, Western European and Others Group (WEOG)

Policy Question(s):

a. What kind of risks that children face related to the level of awareness of their parents and the society?
b. What kind of multi-stakeholder measures can be taken regarding can be taken regarding child online protection (COP)?
c. To what extend, can capacity building and digital literacy guidance improve children's online resilience?

Relevance to Theme: Child safety on the Internet is one of main prerequisite effort to build a healthy digital environment that benefits all. As noted from the discussion of Child Online Protection through Multi-Stakeholder Engagement Workshop at IGF 2015, COP falls into category as one of the most critical issues faced by the world these days.

Children's use of the Internet and mobile technology is increasing, and for many children worldwide there is no clear distinction between the online and offline world. Access to the Internet presents many opportunities for their education, personal development, self-expression, and interaction with others. Yet, the increasingly complex online environment also presents uncountable risks for their safety. Children are prone to be exposed by inappropriate content, harmful interactions, human trafficking, and gadget addiction.

Every parents have responsibilities to be present for their kids both offline and online. To carry out the tasks, parents are required to have enough awareness and knowledge about digital parenting. On the other side, society also bear the same amount of responsibilities to create a safe digital world for all, especially for kids. These heavy tasks cannot be done without all hands joined, hence the multi-stakeholder approach.

Relevance to Internet Governance: This workshop will discuss the responsibility of the multi-stakeholders, especially parents and society, in protecting children online. Invited experts will share their experiences related to this issue. Expected outcomes would be recommendations on how each multi-multi-stakeholder actors can play their roles in making the Internet safe and child-friendly

Format:
Round Table - U-shape - 90 Min

Description: Roundtable setting is used for exploring inputs from both online and onsite contributors. The session will be started with short presentation from each subject matter experts (SMEs), then the floor will be made available for walk-in or remote participants. Discussion highlights will be compiled and put together into more accessible products, such as infographics and short reports which available online, as well as policy recommendation.

Discussion Flow:
- Moderator elaborates the background and introduce all speakers and organisers (5 minutes)
- Each of five SMEs are given the time to present their stance and/or answers to the policy questions (40 minutes)
- Moderator offers onsite and online participants a chance to ask questions or provide statements (30 minutes)

- Each of five SMEs are expected to throw closing remarks or additional statements before closing (10 minutes)
- Moderator concludes the session and wrap things up (5 minutes)
- 90 minutes in total

Some issues to be discussed:
o Principles and norms regarding to COP
o Children's key risks while using the Internet
o Parents' roles in assisting children on the Internet
o How the society be responsibility for children's safety on the Internet
o Best practices of technical and policy approaches on COP
o Capacity building on digital parenting and community engagement
o How children can be well-accommodated during the policy making process and program arrangement related to COP

Expected Outcomes: Reports will be published after the workshop, in the form of conventional text-based scripts and info-graphics. The outputs will be used as one of important tools of policy recommendation and materials for public education in order to raise awareness regarding the issue. Some of the output subjects might be:
a. Principles and norms related to parents and society's responsibilities on COP
b. Action plan that can be done to improve the awareness of parents and the society, especially on digital parenting
c. Binding convention to increase children's involvement in every process of policy making and programs related to the COP

Discussion Facilitation:

Each speaker will be allocated 5-10 minute period to deliver their presentation as introduction to the discussion. The moderator will allow intervention from both online and on-site participants. Then, moderator will invite onsite and online participants to ask some questions to the panelists and/or share their view about the topic

Online Participation:

We will make e-flyer for this workshop, include link for online participation, and promote it to our network in some region. We also encourage our community in Indonesia to join online participation together by arranging the local workshop.

Proposed Additional Tools: We will try to make live streaming through YouTube and Facebook using mobile device

SDGs:

GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 16: Peace, Justice and Strong Institutions

Reference Document

IGF 2019 WS #377 A need for an international digital charter?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):

Human Rights
Internet ethics

Organizer 1: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, African Group
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Theodore CHRISTAKIS, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Flávia Lefèvre Guimarães, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 3: Luiz Fernando Martins Castro, Government, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

Do we need an international digital charter?
What are the fundamental digital rights and freedoms?

Relevance to Theme: Discussions on the need to an international digital charter have impact on the three themes. Nevertheless, at the moment where net neutrality is threatened, it appears important to focus this discussion on the debate on the theme Security, Safety, Stability & Resilience.

Relevance to Internet Governance: Digital transformation represents a vector of progress for humanity, opens up new forms of social interaction and plays an important role in the exercise and awareness of fundamental rights. It also brings in unprecedented innovations that are drastically changing democracy, economy and social interactions. As a common good, steps must be taken to ensure that the Internet operates and evolves in a manner that fulfil human rights to the greatest extent possible.
The realization and upholding of human rights in the digital environment require an inclusive dialogue mobilizing various stakeholders, including the civil society. In this panel, we invite the participants to debate on the protection of fundamental rights in the Digital Age, to envisage forms of guarantee human fundamental rights internationally and mechanisms to ensure the involvement of the civil society in this debate. In this panel, an international charter will be considered to the debate as well.

Format:
Birds of a Feather - Auditorium - 90 Min

Description: This panel will debate the protection of fundamental rights on the Internet, consider an international charter to ensure the guarantee of these rights and envisage some mechanisms to allow the involvement of the civil society.

We will first start this panel by each participant, the French Digital Council, the Brazilian Internet Steering Committee and iRights International, doing a brief presentation about its institutional framework and scope. This first step will allow us to be familiar with each institution and its expertise.

The panel will then focus on fundamental rights in the Digital Age. A first question raises for this debate: Is there a need for an international digital charter in order to ensure fundamental rights on the Internet? We propose to reflect about whether or not an international charter is envisageable and necessary to uphold and advance fundamental rights for the online environment. Jointly with the discussions about a charter, we will also reflect on which rights and principles should be brought to light. This section also invites the participants to think on what form this charter should take shape by defining its aims and willingnesses. In other words, what type of charter do we want? A charter as a reference point for dialogue and cooperation? An authoritative document that can frame policy decisions and emerging rights-based normas for local, national and global dimensions of Internet governance? A policy-making and advocacy tool?

This panel will then focus on representativeness. Bearing in mind that Internet is a common good, how to engage stakeholders, notably civil society, in the debate? What methods, tools and means we can be implemented to coordinate and ensure their participation?

At the end of the panel we will present a brief summary of conclusions and open the debate for a Q&A session.
Agenda:

- Introduction (10 min) by [organizer]

Part I. Presentation of each institution (30 minutes): institutional framework, composition, scope
CNNum (15 minutes)
CGI.BR (15 minutes)

Part II. Debate around the following questions:
How to protect fundamental rights in the Digital Age? Is there a need for an international digital charter?
How do we conceive this charter? What principles should be stated? (40 min)
How to bring representativeness to this charter? (15 min)

Part III.
Conclusion (5 min)
Q&A moderated (20 min)

Expected Outcomes: The but of this session is to propose a draft on an international digital charter.

Discussion Facilitation:

The list below provides examples of the ways discussion and presentation will be facilitated amongst speakers, audience members, and online participants and ensure the session format is used to its optimum: Seating: The panel of experts will debate share their expertise and their vision on Internet regulation sitting at the same table so the participants can see and hear them. It will be an effective way to compare and contrast the various positions of the panel. The moderator will open the discussion with a general review of the policy question and then speakers will provide their remarks on the question and then address questions from the moderator. At least 30 minutes will be allowed for questions/comments from the audience.

Media: The organizers will explore the use of visuals (i.e. PowerPoint slides, images,) to animate the session and aid those whose native language may not be English. Experts who have short video material to share will be encouraged to help animate discussion and debate on these examples. Video material may also be considered to help engage remote participants.

Preparation: Several prep calls will be organised for all speakers, moderators and co-organisers in advance of the workshop so that everyone has a chance to meet, share views and prepare for the session. Cgi.Br and CNNum will met during ICANN at Marrakech to discuss on this panel.

Moderator : Nicolas Chagny is an expert in digital policy and experienced in animating multistakeholder discussions. He has been appointed in 2019 in the French National Consultative Commission on Human Rights (CNCDH).

Online Participation:

The remote moderator will be involved throughout workshop to include participation from online viewers. The onsite moderator will frequently communicate with the remote moderator during the session to ensure remote participants' views/questions are reflected and integrated to the discussion, specially suring the Q&A sequence. This will ensure remote participations are given the opportunity to interact with multiple experts remotely. Organizers have specially invited a participant to act as the remote moderator and will share information with the remote moderator about training sessions for remote participation at IGF and ensure they have all the necessary information. Co-organizers will ensure that the workshop is promoted in advance to the wider community to give remote participants the opportunity to prepare questions and interventions in advance. We can include the intervention from youth participants from Latin America and Africa to increase diversity and bring fresh opinions and questions to the debate. Any handouts prepared in

advance for the panel will be shared with remote participants at the start of the session so that they have the necessary material to participate.

Proposed Additional Tools: Given the varied background of discussants and audience members, organisers will explore introducing questions to animate discussion on social media in the run up to the workshop. This will introduce the subject, encourage conversation and create links to other dialogues on digital skills taking place in other forums to create awareness and help prepare in-person and remote participants for the workshop.

SDGs:

GOAL 1: No Poverty
GOAL 2: Zero Hunger
GOAL 3: Good Health and Well-Being
GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 6: Clean Water and Sanitation
GOAL 7: Affordable and Clean Energy
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 11: Sustainable Cities and Communities
GOAL 12: Responsible Production and Consumption
GOAL 13: Climate Action
GOAL 14: Life Below Water
GOAL 15: Life on Land
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #383 The human-side perspectives to Internet safety and security

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Democratic Values
Human Rights
Trust and Accountability

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, African Group

Speaker 1: Anri van der Spuy, Civil Society, African Group
Speaker 2: Kenneth Adu-Amanfoh, Government, African Group
Speaker 3: Matthew Shears, Civil Society, Western European and Others Group (WEOG)
Speaker 4: Mallory Knodel, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

The round table's primary policy question is to explore what policy research tools do policy makers have to go beyond the normative and technical aspects of cybersecurity and data protection by promoting a better understanding of Internet users' needs and perceptions of their privacy, safety and security online. The aim is to provide policymakers and other practitioners with practical guidance on how to include a human

perspective to internet safety and security, in order to support the development of an Internet that can foster economic growth while reducing cyber-risks and harms, and sustainable development on the African continent and beyond.

In order to answer to this main question, the secondary questions are:

Do policy-makers take into account the human-rights dimension of data protection and cybersecurity when they develop policy and regulatory frameworks related to security, safety, stability and resilience?

What are the developmental challenges related to cybersecurity and data protection in Africa?

Do policymakers in Africa have enough capacity to investigate human issues related to security, safety, stability and resilience? What are the resources and tools available to build such capacity?

How can we measure and quantify potential progress to improving security, safety, stability and resilience in cyberspace to achieve the SDGs?

What societal, political, economic and capacity structures would need to be in place to effectively include a human-centric perspective to cyber-policy development?

How can we identify and quantify potential harms caused by cyber-threats and cyber-crime?

What are the existing norms that can bring about a human-centric approach, how practical are they and how can they be implemented by policymakers?

If the Internet is a “trust” technology, people’s views change significantly as they become more frequent users - how to account for this in long-term planning?

Relevance to Theme: Country’s approach to cybersecurity is a critical enabler for the achievement of the SDGs, in particular for #16 “[p]romot[ing] peaceful and inclusive societies for sustainable development, provid[ing] access to justice for all and build[ing] effective, accountable and inclusive institutions at all levels”.
Other goals relating to the human-side of cybersecurity are to ensure participation in economic processes and build trust in Internet-based services (SDG #1), to provide access to health services, which protect individuals’ personal information and guarantees the resilience of health services (SDG #3), to protect vulnerable groups (in particular women) against any online based discrimination and to foster their inclusion (SDG #5), and to give everyone access to Internet-based education and the adequate skill set, as well as raising the awareness of cyber risks (SDG #9).

Relevance to Internet Governance: Internet governance is a multistakeholder forum which brings different perspectives relating to specific issues affecting the development of the Internet. Therefore, the IGF is the right venue for discussing the issue of the human-side on cybersecurity, because the multistakeholder approach to the theme allows different perspectives to be brought into the discussion, beyond the technical and normative approach which normally underlines cyber policy development.

Format:

Round Table - U-shape - 60 Min

Description: During the roundtable, the notion of a human-centric approach to cyberpolicy will be untangled. To distinguish between a traditional, normative, and technical approach to cyberpolicy, the panelists will be invited to discuss methods and approaches to bring in a people-centred perspective in the policymaking process.

The debate has the following intended agenda:

Introduction to the topic of a human-centric approach to cyberpolicy, and a brief introduction of the discussants;
Presentation of #AfterAccess data pertaining to African users awareness on privacy, and safety and security

online;
Debate on research findings moderated by the RIA Principal Investigator on cybersecurity;
Open microphone for online and offline interventions and questions from the public;
Answers from the discussion;
Wrap-up and takeaways.

Expected Outcomes: Research ICT Africa is currently conducting research on this topic through its Africa Digital Policy Project (ADPP), which focuses specifically on cyber policy challenges for Sub-Saharan Africa. The intended outcomes of this workshop proposal are related to one of the ADPP aims which is to provide African stakeholders with the information and analysis required to develop innovative and appropriate cyber policies better able to address the challenges of sustainable development on the continent. The workshop is expected to facilitate evidence-based and informed cyber policymaking for supporting the development of an Internet that is free (based on and supportive of human rights), trusted (based on sound cybersecurity measures), and innovative (based on enabling policy environments).

Discussion Facilitation:

The moderators (offline and online) supported by the round table organisers, will involve discussants and the public in the debate, and will facilitate the discussion on the topic of the round table. Specifically, in order to optimise the time and to assure fair participation of both online and offline participants, the debate will unfold in the following way:
Suggested Agenda (60 minutes):
a. Opening: presentation of the round table and policy questions (5 minutes)
b. Panelist remarks (5 minutes each: 25 minute in total)
c. Discussion (15 minutes), including comments and questions from remote participants
d. Closing remarks from panelists (2 minutes each: 10 minutes in total)
e. Wrap-up (5 minutes)

Online Participation:

As recommended by the MAG, the organising committee of the Round table will train an online moderator who will assume responsibility for giving online attendees a separate queue and microphone, which will rotate equally with the microphone in the room. The on-site moderator of the round table will keep the online participation session open and will be in close communication with the workshop's trained online moderator to share the online questions and interventions in the on-site room. The trained online moderator will collect opinions, questions and comments during the roundtable and the most relevant contributions to the discussion will be shared among the participants to the roundtable.

Proposed Additional Tools: YES through Twitter and collaborative editing on pads (https://pads.riseup.net)

SDGs:

GOAL 1: No Poverty
GOAL 3: Good Health and Well-Being
GOAL 5: Gender Equality
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #385 Combating New Threats to Cyber Security-Indian Perspective

Theme: Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Cyber Security Best Practice
Human Rights

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Private Sector, Asia-Pacific Group
Organizer 4: Civil Society, Asia-Pacific Group
Organizer 5: Civil Society, Asia-Pacific Group
Organizer 6: Civil Society, Asia-Pacific Group

Speaker 1: Arnab Bose, Civil Society, Asia-Pacific Group
Speaker 2: Seema Sharma, Private Sector, Asia-Pacific Group
Speaker 3: Prathik Karthikeyan, Civil Society, Asia-Pacific Group

Policy Question(s):

Q1) How can cooperation and collaboration on national, regional and global levels help to increase cybersecurity?
Q2) What legal regulations are already in place but potentially need to be enforced and what new legal regulations should be created to address upcoming threats?
Q3) The possible application of blockchain in the prevention of fraud and data theft as well as the capacity for Machine Learning and Artificial Intelligence be used in the field of cybersecurity?

Relevance to Theme: The Policy paper addresses the key gaps in cybersecurity policy in India by focusing on suggestions with regards to increasing international as well as regional cooperation to increase information sharing and technical information and aid in the dissemination of similiar mechanisms at the regional and sub-regional levels. The presentation will also critically analyse India's Draft Data Protection bill and identify gaps in it and policy suggestions that would not only be useful to incorporate not only in the Indian context but also among other developing countires in their legaslation on data protection and cybersecurity. We will also delve into the questions of utilisation of Machine Learning and Artifical Intelligence and blockchain in bolstering cybersecurity.

Relevance to Internet Governance: The policy examines the ways in which India's Draft Data protection bill affects the civil society,private sector as well as the citizens of the nation. It also proposes new policy measures for intergovernmental cooperation on the international and regional levels through existing mechanisms as well as regional versions of these mechanisms like the UN IMPACT, so as to increase cooperation and technical knowhow.

Format:

Other - 60 Min
Format description: A fishbowl type workshop with a group discussion at the end:
Wherein first the audience witnesses an interaction between two viewpoints of the policy proposal as well as a comprehensive discussion on the subject matter, which will be followed by observations as well as general comments by the audience and any possible suggestions or changes that they may suggest finally concluded in a summary discussion by the presenters including the points brought up by the audience and formulate and solidify policy.

Description: The Policy paper addresses the various ways in which we can increase intergovernmental cooperation. It will also look into the Draft Indian Data Protection Bill and extrapolate the measures and safeguards that should be present in data protection laws. Finally, we'll examine the relevance of new technologies like blockchain and artificial intelligence in the field of cybersecurity.

Expected Outcomes: To critique the Indian Data Protection Bill and identify the safeguards and gaps that we should be wary of in data protection laws, as well as gain a deeper understanding of intergovernmental cooperation in the field of cybersecurity and review policies with regards to the emergence of new technologies and their relation to cybersecurity.

Discussion Facilitation:

Use the fishbowl method to allow the audience to gain a nuanced understanding of the topics discusses, questions will be encouraged to be asked during the session or have questions posed towards the end as well. Participants will then be invited to talk about possible policy suggestions as well as critiques to the proposed policy decisions. At the end of the discussion, the presenters will make a summary with regards to the discussion and taking into account the proposed changes and critiques and hopefully reach a consensus on the policy.

Online Participation:

Make use of the online live streaming service and have questions as well as suggestions posed through an online questionnaire.

SDGs:

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities

Reference Document

IGF 2019 WS #392 Are anonymous forums leading us to a less tolerant society?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Anonymity
Harmful Speech
Human Rights

Organizer 1: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 2: Civil Society, Latin American and Caribbean Group (GRULAC)
Organizer 3: Civil Society, Latin American and Caribbean Group (GRULAC)

Speaker 1: Dajana Mulaj, Civil Society, Eastern European Group
Speaker 2: Rebecca Ryakitimbo, Civil Society, African Group
Speaker 3: EDUARDO MAGRANI, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 4: Martin Fischer, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

The Policy Questions will be addressed in two groups -- Stage 1 will set the debate over the first third of the workshop, while Stage 2 will be more open-ended, allowing for a much greater degree of audience participation. The structure is explained in details further in the proposal.

Stage 1
In what ways online anonymity in platforms such as discussion forums can be, and is used, towards

legitimate, lawful purposes compatible with human and constitutional rights?
To what extent are anonymous forums contributing to violent extremism, radicalization and harmful speech in societies across the globe?
To what measure is the harmful speech displayed in anonymous forums illegal, as opposed to merely distasteful, when considered under an international perspective of multiple countries and their regulations?
In a situation of anonymous harmful speech, how does the individual's or group's intentions and age affect our judgement? Does age play a factor in liability? Do exclusively satirical intentions or political debate trump what would otherwise be harmful content?

Stage 2
Are anonymous platforms otherwise compliant with national regulations, and do they function as regular private sector businesses?
What technical measures can be adopted by the stakeholder groups to minimize the negative impact of anonymous platforms and maximize their positive impact?
Do anonymous platforms require specific regulation? If yes, how should State actors balance it as to not intrude on lawful freedom of speech and online business models? How would it affect other platforms?
What non-regulatory means are available to State actors to effectively, proportionally respond to crisis relating to anonymous spaces, keeping in mind a perspective of minimal interference towards the lawful enjoyment of human rights?

Relevance to Theme: While Safety and Resilience often refer to technical aspects of the network, we can also apply it to the physical safety of users and their psychological resilience, as stated in the Theme's description. This workshop aims at exploring this exact point, in the specific context of online anonymous forums and their possible relation with violent radicalization, harmful speech, political extremism and echo chambers.
As an inciting incident, linking those forums to unlawful acts, we can pick the recent New Zealand Christchurch shooting, which so far has been related to a specific online anonymous image board (8chan) in which the shooter announced his manifesto and gave out the link for the shooting's livestream. As of the writing of this document there are 49 dead, painting a bleak picture of how online extremism can lead to a loss of life.
We don't need, however, to exclusively look at violent crimes. Those anonymous image boards can be studied for their extreme content on its own, as well from how they are a means to fully realize freedom of expression for those who would be harmed for their opinions. In this sense, anonymity when coupled with freedom of expression seems to be a two edged sword; it can save the life of the dissident who would be persecuted for his beliefs, as it can cultivate an environment of non-accountability for one's harmful content.
We can trace comparisons between anonymity in this area with how it can play out in the WHOIS system. While in Europe WHOIS anonymity is seen as a matter of privacy, in undeveloped countries an activist's identity can be revealed with a simple online search which can lead to both social and physical harm.
The subject of how those image boards lead to radicalization and violence is made imperative in spaces like the IGF, where the matter can be appreciated under many perspectives. In this proposal so far we've focused on how it impacts the users' security and resilience, but there are direct implications to the Web's Resilience as well -- in response to the Christchurch shooting, New Zealand authorities responded by blocking two anonymous image boards (4chan and 8chan), a video-sharing site (Liveleak) and went on to ban possession of the shooting's video under Possession of Objectionable Material, with a possible jail time of 10 years.
In this sense, we can state this workshop's connection to the Theme of Security, Safety, Stability and Resilience is twofold; mainly it relates to the users' integrity, and secondarily to how countries can respond to threats relating to anonymous forums in ways that do not harm Internet's integrity.

Relevance to Internet Governance: In enjoying the right to freedom of speech, anonymity can be an important shield in defending individuals who, holding on to unpopular opinions, would be harmed by an intolerant majority. It can help ethnic and religious minorities who would have their integrity harmed by totalitarian governments or paramilitary groups. Similarly it can protect those who hold on to unpopular, but otherwise harmless, political opinions, or who identify with, for example, sexual minorities with whom association would cause damage to one's career. In all those circumstances, anonymity comes up as a facilitator to the full realization of one's freedom of speech.

Notwithstanding, anonymous forums are, in a way, conducive to the new wave of privacy protecting regulations worldwide, in the sense that they ultimately abdicate on the requirement of offering any data before gaining access to it.
Simultaneously, anonymity can instill a wide array of harmful behaviors, both to individuals and to the world at large. By often instilling a sentiment that one's actions cannot be traced back, it can be a breeding ground for harmful speech and extremism, which can lead to anonymous communities gradually turning into echo chambers and catalysts for further radicalization.
This phenomena has implications for all of Internet Governance's stakeholder groups. The use of anonymity as a catalyst for freedom of speech and hate speech is a matter of pertinence to civil society, who has a stake on both sides.
Bringing the issue to the discussion of elections, the popularity which Donald Trump achieved among anonymous forum users is considered an important factor for his victory, and anonymity is a conducive tool for the dissemination of fake news both by interested individuals and hired actors. When coupled with those environments' potential to radicalize, such as what has been observed in the recent Christchurch shooting in New Zealand, which has been associated with an anonymous forum, it becomes an urgent matter. Austria has announced they want to enforce identification for Austrian internet users in large platforms, as an attempt to curb hate speech. Suffice it to say that governments, too, have a stake in this debate.
The private sector also has a stake in this matter. Microsoft's TayAI initiative was derailed by an effort originating from an anonymous forum, which consisted in feeding the AI's algorithm with hateful speech. Those forums' tendency towards disruption can be an issue. Those websites are, however, ultimately platforms like any other; would an attempt at regulating them affect other social media businesses? This questioning by itself warrants bringing the private sector to the table, as ultimately it is also a question which can impact other platforms.
When it comes to the technical community, anonymous forums are an environment whose principles hark back, at times, to a cyberoptimistic perspective, to the shedding of national identities, which by itself can be an attractive to technical communities which would prefer to keep its members' identities unknown.
This discussion is particularly appropriate for the IGF as it benefits greatly from a global perspective. The very definition of hate speech is country-dependant, and even an approach based around harmful speech is heavily dependant on cultural differences. When applied beyond the initial issue of freedom of speech, we can assess its implications both on democracies, in how those forums can act as breeding grounds for malicious efforts, and in the safety of people who might be victimized by radical actors instilled by anonymous echo chambers.
In this context, anonymous forums come up as an uniquely relevant type of platform, in that their specificities bring about a mix of old and new issues, given new relevance.

Format:

Round Table - U-shape - 90 Min

Description: The Policy Questions will stand as the main pillars of the debate. They are divided into two groups.
Stage 1 Questions are brief and direct, meant to set the stage for the debate. Each Speaker will be given one question, tailored to their expertise and experience. After a 4 minute speech from each of them we'll have our first opportunity for interventions, when the audience will be able to complement the basic discussion so far, offering their own answers to the policy questions, or challenge what has been stated.

Afterwards we'll have the Stage 2 Questions, which are more complex and offer a greater space for debate. They all have a strong component of practicality and try to raise debate about what each stakeholder group can do to improve the situation. Once again each Speaker will be given a question, tailored to their expertise.

Afterwards we'll have the main moment of the workshop, 20 minutes of open debate in which the audience will be able to offer their own insight into the questions. We consider that it'll be through this open debate, built upon the Speakers' initial points, that we'll be able to achieve the outcomes described below.

We have set aside 10 minutes for the Speakers to respond to the Open Debate, and further 5 minutes for concluding Remarks. This structure is satisfactory but, notably, flexible; should the debate be too fruitful and

intense we can cut down on Concluding Remarks, and so can we merge the Speaker Responses into the Open Debate itself.

We leave 5 minutes aside as a safeguard against delays and, should none occur, extra time for discussion.

Introduction (4 minutes)
Stage 1 Questions (4 minutes for each question, total of 16 minutes.)
First Audience Q&A (10 minutes)
Stage 2 Questions (5 minutes each, total of 20 minutes.)
Open Debate Part 1 (20 minutes)
Speaker Respond to Open Debate (10 minutes)
Concluding Remarks (5 minutes)
Time for Delays: 5 minutes
Total Time: 85 minutes + 5 for Delays.

Expected Outcomes: This workshop aims to bring together people from all different regions, stakeholder, and organizations to have a face-to-face discussion about the impact of videogames communities and anonymous forums have for dissemination of harmful speech among youth.

The session will address three main issues that are central for the discussion (i) the impact of anonymous communities for youth social insertion on the Internet, (ii) the impact of these communities for dissemination of hate speech online and offline and (iii) how regulation and Internet policies can address this issue.

While it is difficult to measure the exact impact of these communities for the socialization of young people on the Internet, the current scenario indicates that many of the participants are young and many of the young people involved with hate crimes are also part of these communities. This session, therefore, has as a goal to increase the debate around the topic, pointing out some of the questions that still need to be analyzed.
Speakers and participants will address the following trigger questions:
How is the Internet changing the nature of relations between youth and how their socialization through videogames and anonymous communities occur? How are these communities strcutured? How does their structure facilitate the dissemination of hate speech? What is the actual impact of it on offline and online hate attacks? How should Internet policies address it, given that anonomity is an essential tool for privacy and freedom of expression?

By addressing those issues we hold the following points as our expected outcomes:
a. Assessing the pros and cons associated with anonymous discussion forums and platforms;
b. Achieving a consensus about the issues that require addressing from the stakeholder groups, in particular regarding harmful speech and radicalization;
c. Assessing how youth contributes and is affected by those discussion forums;
d. Assessing possible responses and plans of action for how stakeholders can minimize negative impacts, and
e. Establishing how regulation can play a part in this debate, and how it may relate to platform regulation in general.

Discussion Facilitation:

As described in the Workshop Session Description field, this proposal has as a central point two periods in which the audience will have, overall, 30 minutes to actively participate so they may build effectively reach a consensus. We have outlined a two-stage structure for this, in which the first period of the workshop deals with "setting the stage" and making sure all are up-to-date on the current state of affairs. The participants will have an opportunity to intervene then.
On the second period, after 20 minutes of Speakers answering pre-determined central questions, the participants will have a minimum of 20 minutes to engage with the questions and answers provided.
There're 15 minutes afterwards scheduled for final Speaker remarks and a Conclusion, which can be

reallocated in favor of incentivizing participation should the debate be particularly fruitful.
This is why we have selected the U-Table format, as it allows for interested participants to engage directly via the microphones -- as opposed to requesting an opportunity to the moderator.
The structure of this roundtable is intended to foster an inclusive conversation and promote constructive exchanges between participants and speakers.

Online Participation:

In order to promote an effective discussion on the proposed topics between onsite and online audience and to allow interventions, online participation will be facilitated as mentioned above, as well as via the Youth Observatory online discussion forums.
The opportunity for Q&A will also extend to remote participants, who will be given the opportunity to ask questions through the dedicated online forum.
All of the session organizers have abundant experience managing remote participation in the Youth Observatory and ISOC context and will have no trouble facilitating remote participation.

Proposed Additional Tools: In addition to the aforementioned fora, we will also promote a dedicated hashtag so that the panelists, audience members, and online participants can discuss the issues raised in real time on a more widely accessible medium.
A collaborative document will gather these records of comments and questions during and after the workshop, to be later integrated into the report. A variety of media can also serve as background material for this debate, based on previous workshops. Remote participation tools will ensure an inclusive, accessible, and global audience both via the IGF online participation tools and Youth Observatory online discussion forums.

SDGs:

GOAL 5: Gender Equality
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #402 Progressive Policies for Digital Media

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Fake News
FoE online
Hate Speech

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group
Organizer 3: Civil Society, Asia-Pacific Group
Organizer 4: Civil Society, Asia-Pacific Group

Speaker 1: Asad Baig, Civil Society, Asia-Pacific Group
Speaker 2: Qurratulain Zaman, Civil Society, Western European and Others Group (WEOG)

Speaker 3: Xianhong Hu, Intergovernmental Organization, Western European and Others Group (WEOG)

Policy Question(s):

What are the key enablers and challenges to digital freedom of expression? How are cyber-security regulations affecting the development of digital news media ecosystems? How are regulatory regimes

affecting the online media freedom of journalists? How have online threats to the safety and security of digital journalists translated into offline threats and harm, and how can policy and legal protections help in this regard? What are problems attached to the implementation of policies that can be considered progressive and what are possible solutions? What role should Internet platforms play in defining the standards for acceptable content in light of freedom of speech? Should Internet platforms take into account cultural and religious factors when defining these standards? How can online risks and threats to women journalists be reduced through regulation and technology? How can feminist principles of the Internet advise in protecting the online media freedom? How can the clash between cultural relativism and the right to free speech be prevented? How does the freedom of expression for journalists be weighed against the freedom of speech demanded by far-right extremist groups? How can tech platforms support innovation in the digital news media? What kind of collaboration could be created among Internet platforms and media outlets to fight disinformation and fake news?

Relevance to Theme: The proposed workshop session will look at the risks to the security and safety of online journalists to identify ways in which resilience can be built in digital journalism networks around the world. It will also allow for discussions on the role of technology platforms and governments in protecting online freedom of expression. The session is relevant to the theme due to its focus on safety of a specific kind of Internet users – journalists – and the stability and resilience that is required in systems through policies and laws to help journalists feel secure.

Relevance to Internet Governance: The proposed workshop session will encourage discussion on collaboration between government, civil society groups, and technology industry to arrive at shared principles and decision-making procedures to protect freedom of expression online at the same time as discouraging the spread of disinformation through social media platforms. In terms of the use of the Internet for ensuring the rights to free speech and free press, the discussion will be highly relevant to the spirit of Internet governance.

Format:

Panel - Auditorium - 60 Min

Description: Around the world, journalists and news organizations have turned to digital media, including social media platforms, to inform their audiences and show truth to power. Even though examples of digital news media innovation have been observed in various parts of the globe, more common and consistent are the threats that journalists now face online. From coordinated trolling campaigns to doxxing of their personal data, digital journalists are faced with a new set of risks that force them towards self-censorship. In many instances, physical attacks on journalists have been reported after they had been subjected to online harassment and abuse. Women reporters and journalists from marginalised communities are especially subjected to hate online. At the same time, the community standards of social media platforms and government laws on cyber-security have failed to adequately protect the journalists. In this context, the proposed panel discussion will look at the foremost issues facing the online news media while acknowledging the attempts at digital innovation. The workshop session hopes to identify the progressive action required from governments and technology companies in terms of laws and policies that will allow for better protections for online freedom of expression. The panel discussion will feature brief talks from four speakers who have worked closely on media freedom and digital media innovation in different parts of the world. Following the talks, the moderator will lead an interactive discussion with the speakers and participants to provide answers for some of the policy questions related to the online freedom of expression debate. The agenda of the proposed workshop session is as follows: Introduction (Moderator, 3 minutes) – The moderator will introduce the session and the speakers before briefly sharing the agenda. Talk # 1 (Speaker # 1, 10 minutes) – Speaker Gayathry Venkiteswaran (University of Nottingham Malaysia) will talk about the state of online media freedom in the Asia Pacific region and the way state policies and attitudes are affecting the journalists. Special focus will be on the cultural and religious factors that obstruct online press freedom in the Asia. Talk # 2 (Speaker # 2, 10 minutes) – Speaker Asad Baig (Media Matters for Democracy, Pakistan) will speak about the use of social media by journalists in the South Asian region, the threats they have been exposed to as a result, and the kind of support online freedom of expression requires from social media platforms and governments. Mr. Baig will also focus on the experience of women

journalists in India and Pakistan who have had to face coordinated online campaigns that discredited their journalism and sometimes also used deep fakes to malign their character. Talk # 3 (Speaker # 3, 10 minutes) – Speaker Chirinos Mariengracia (Institute Press and Society Venezuela) will speak about the monitoring of digital freedom of expression in South America and will share the risks of online expression to journalists in the Americas. Talk # 4 (Speaker # 4, 10 minutes) – Speaker Qurratulain Zaman (DW Akademie) will speak about her report on digital innovation for DW Akademie and share insight on how digital innovation can be used to counter some of the digital threats to journalists. Q&A session (Speakers and participants, 15 minutes) – The moderator will take questions from the audience and request the speakers to respond. The moderator will also quickly connect the questions and responses with policy recommendations. Thank you note (Moderator, 2 minutes) – The moderator will briefly recap the conversation and thank the participants and speakers.

Expected Outcomes: The expected outcomes are given below: 1 An identification of the diverse and evolving challenges to online freedom of expression. 2 Discussion on the effectiveness of digital innovation in protecting online freedom of expression. 3 Recommendations for progressive policies to ensure that the online freedom of expression of journalists is not compromised.

Discussion Facilitation:

Interaction and participation will be incorporated by devoting a quarter of the session time to a Q&A session with the audience. Online participation will also be ensured with the help of the online moderator who will field questions from the online participants and share them with the moderator to seek responses from the participants.

Online Participation:

Remote participants will be able to follow the talks by the speakers and will be able to participate in the Q&A session with the help of the online moderator.

Proposed Additional Tools: The online moderator will use Twitter to share the salient points from the talks of the speakers and the comments during the Q&A session.

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #403 IPv6 Independence Day: Rest in peace IPv4

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Internet Protocols
Internet Resources
IPv6 deployment

Organizer 1: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 2: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 3: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 4: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 5: Technical Community, Latin American and Caribbean Group (GRULAC)
Organizer 6: Technical Community, African Group
Organizer 7: Civil Society, Asia-Pacific Group
Organizer 8: Technical Community, Latin American and Caribbean Group (GRULAC)

Speaker 1: Adarsh Umesh, Civil Society, Asia-Pacific Group
Speaker 2: Antonio Marcos Moreiras, Technical Community, Latin American and Caribbean Group (GRULAC)
Speaker 3: Mukom Akong Tamon, Technical Community, African Group

Policy Question(s):

The discussion in the proposed session will be facilitated around four policy questions posed for the participants in the round-table as well as the audience in general:

(1)When it would be the ideal time to stop using IPv4? What would be the ideal conditions to indicate that the appropriated time has arrived? Will we need some kind of enforcement for this situation?

(2) How do we prepare technically, politically and economically for this day? How can multi stakeholder approach help on that preparation? What role each stakeholder would play on that transition?

(3) How do we plan this transition without affecting Internet Governance principles, taking into account the security, stability and resilience of the Internet?

(4) Can we use some similar successful examples like the DNS root KSK rollover practices for the IPv6 migration? Or the practices of another similar case?

The on site moderator will be in charge of presenting the questions, ensuring that all the speakers and people in the audience can expose their ideas as well as encourage discussion.

Relevance to Theme: This submission is related to the security, safety, stability and resilience theme.

It is well known that IPv6 was developed to someday replace IPv4 in Internet communications. However, when this day comes, will we be prepared?

In an attempt to maintain the stability of the Internet, most networks nowadays are moving towards operating with both IPv4 and IPv6. According to measurements made by such relevant Internet companies as Google, Akamai and Cisco, more than a quarter of the Internet traffic is already running on IPv6. In fact, those measurements suggest that IPv6 usage may reach around fifty percent in a few years. However, should we wait until it is almost too late for this transition to then start preparing for it? In other words, what should the threshold for IPv6 deployment be to support the shutdown of IPv4: 80 percent, 90 percent, 99 percent, or only when we reach 100%?

Answering this question is not an easy task because it will affect all the Internet! If a part of the Internet does not migrate to IPv6 and continues working with IPv4-only, it will be isolated when this shutdown happens. That part of the Internet will be like an island on the network. The Internet users from that island will not be able to communicate with the rest of the Internet and vice versa. Additionally, we could experience exclusion if part of the Internet decides to shut down IPv4 alone. Except that in this case, an IPv6-only island will be created, thus alienating the rest of the world which has not fully deployed IPv6. In other words, a joint effort of all stakeholders is essential to solve this situation. All of them must work together to migrate networks to IPv6-only and decrease and avoid negative effects.

Analyzing the issues involved in the transition from IPv4 to IPv6 is the focus of this workshop. This analysis is particularly important because this transition might cause serious troubles for the whole Internet such as isolation, digital alienation, lack of stability and security complications.

The Internet is composed by a mesh of connections among autonomous systems (Service provider, Content provider, Transit Provider). If one of these autonomous systems establishes only one protocol (IPv6 or IPv4) to use while others are using the other protocol, it will be apart from the network (an isolated island). Its users would not have access to all services and information available on the Internet, and this would infringe one of the basic Internet Governance principles (that of the freedom of information and access to information).

Besides, this island might prove even more serious if it is located in the core of the Internet (Tier 1 or Tier 2). This issue would reduce the amount of paths on the Internet. Packages would have fewer routes to reach their destinations, thus having a negative impact on the stability and resilience of communication causing packet loss and higher latency. In addition, security and privacy issues may happen because of the path reduction. The absence of a safe route can force packages to follow unsafe paths.

A parallel can be made with the DNS root KSK rollover process that involved several stakeholders. During the exchange of keys some networks were isolated and their users lost access to the internet. Much of what has been learned can be applied in this migration of protocols.

Therefore, it is important to prepare for the moment when IPv4 will definitely stop from being used. Only through a discussion of this problem in a multistakeholder, interdisciplinary and international context, a comprehensive solution will be achieved.

Relevance to Internet Governance: The Internet was created and developed with the Internet governance principles of freedom of association, information and access to information. To achieve these goals services, applications and infrastructure needs to work properly. If one part fails, the whole structure will be compromised.

This workshop will discuss the implications that Internet might suffer when disconnecting IPv4, especially if a joint effort with all stakeholders does not happen.

For more than 30 years the Internet has used IPv4. However, the amount of free IPv4 public addresses that can be allocated to machines are depleting. According to some studies made by Regional Internet Registries (RIRs), it is expected that in less than 5 years there will be no more IPv4 public addresses to be assigned. In other words, IPv4 needs to be replaced by its successor IPv6.

At this moment, networks are concentrating efforts in working with both protocols (IPv4 and IPv6). However, working with both generates a lot of wasted efforts. On the one hand, developers spend their time and energy developing identical functions for the two protocols. On the other hand, network devices share their memory and operations to handle packets of the two protocols. So this is a temporary solution until it is possible to shut down the IPv4.

In order to shut down the IPv4, a joint effort with all stakeholders is necessary. Not only to ensure the correct operation of the Internet (including the Internet governance principles) but also to minimize problems that may happen. Especially because, as explained in the text “Relevance to Theme”, islands (IPv4 and IPv6) on the network may appear, causing trouble to stability, security and resilience of the Internet.

Each of the stakeholders needs to understand their role in this transition to ensure the least impact on the whole Internet.
Internet Services Providers (ISPs) are responsible for providing Internet access to theirs customers. Regardless of the protocol they use (IPv4 or IPv6), they must ensure that their users have access to the entire Internet. If they decide to operate with only one protocol without the help of other stakeholders, they may lose access to part of the Internet. This will violate the principles of Internet governance and will cause a drop in their revenue due to the number of customers that will decline their services.

Manufacturers develop network devices to allow users to communicate with a service on the Internet. These devices nowadays need to operate with both protocols, especially because this is a requirement of the current market. If manufacturers develop their devices with no support for a protocol with a demand from other stakeholders, this may lead to a decrease in their sales.

The governmental responsibility is to create regulations to guarantee the rights of users and companies that depend on the Internet. However, legislating on which protocol should be used in a country without the support of the rest of the world is a very risky situation. The regulation may cause a digital exclusion of the country besides harming the economy. Many companies can move their operations to other countries because they do not accept the new regulations.

Academia, research groups and standards organizations (like IETF) have an important role in disseminating knowledge and developing Internet protocols. As both IPv4 and IPv6 are being used on the Internet, they should not state just one protocol to be taught to the community, as the lack of knowledge of the other protocol can generate a difficulty in finding qualified professionals to meet market demand. Such situation may affect the economy causing an inflation of the prices of products and services on the Internet.

Therefore, it is fundamental to bring together different actors involved in migrating protocols to discuss the issue in order to advance comprehension of this problem and identifying possible solutions in order to satisfy different perspectives.

Tag 1: IPv6 deployment
Tag 2: End of IPv4
Tag 3: Migration from IPv4 to IPv6

Format:
Round Table - U-shape - 90 Min

Description: The session is structured in three 30-minute segments. The first segment will be a presentation of the mini résumé of the speakers as well as an introduction on the general topic made by the moderator. He will summarize his briefing by posing a question to the participants. The question will be related to IPv6 deployment and IPv4 address exhaustion observed in different regions and companies. A 20-minute segment will follow in which participants in the round-table will be able to make 3 or 4 minute interventions, one at a time.

In the second 30-minute segment, the moderator will will encourage discussions through the 4 policy questions presented in this document. He/she will provoke participants to look into the future when the Internet will migrate completely from IPv4 to IPv6. Another 20-minute segment will follow in which participants in the round-table will be able to make 2 or 3 minute interventions at a time.

The last part of the session will comprise a 30-minute open mic session that will be based on a topic that delves into “the role of the multistakeholder community to help this migration." The last five minutes of the third segment will be used by the moderators to summarize discussions.

The workshop speakers are:
Mr. Klaus Nieminen (Ficora, Government, Finland) - TBC
Mr. Lee Howard (Retevia, Private Sector, United States of America) - TBC
Mr. Antonio Marcos Moreiras (NIC.br, Technical Community, Brazil)
Mr Adarsh Umesh - (Rural Development SIG, Civil Society, India)
Mr Mukom Akong Tamon (Afrinic, Technical Community, Cameroon)

Agenda:
The session is structured in three segments.

First segment
10 minutes - Presentation of the mini résumé of the speakers and a general introduction about the topic under discussion
20 minutes (up to 4 minutes each panelist) - Round table - their points of view about IPv6 deployment and IPv4 address exhaustion observed in different regions and companies

Second segment
30 minutes (up to 6 minutes each panelist) - Round table - to discuss all the 4 policy questions

Third segment
25 minutes - open mic session, to engage the audience and the remote participants to discuss the topic that delves into “the role of the multistakeholder community to help this migration.
5 minutes - used by the moderators to summarize discussions

Expected Outcomes: The idea behind the session is to promote, in an international and collaborative environment, a discussion about the future of Internet infrastructure. Although it is very widespread that IPv6 will replace IPv4, it is hardly discussed when this will happen or how to prepare for this moment. It is important to emphasize that this is not an easy transition and that all multi stakeholders must collaborate to avoid problems on the Internet.

Finally, it is expected that after all the discussions presented at the workshop this will increase the concern about the theme and it helps to get more people engaged in the migration to ipv6. Only through the support and knowledge of all multi stakeholders, this transition can happen with the least impact for the Internet.

Discussion Facilitation:

The discussion will be facilitated by the on site moderator who will guide the debate in each of the proposed segments for the workshop as well as during the Q&A and comments session in the end. The online moderator will make sure the remote participants are represented in the debate.

Online participation and interaction will rely on the WebEx platform. Those joining the session using WebEx (either invited members of the round-table or the general audience) will be granted the floor in the open debate segment of the workshop. People in charge of the moderation will strive to entertain onsite and remote participation indiscriminately. Social media (Facebook, but not Twitter or Reddit, since they do not support IPv6) will also be employed by the online moderators who will be in charge of browsing social media using hashtag (to be defined).

Lastly, having two moderators will facilitate the control of time, which will be very important for the proper functioning of the workshop.

Online Participation:

Online participation and interaction will rely on the WebEx platform. Those joining the session using WebEx (either invited members of the round-table or the general audience) will be granted the floor in the open debate segment of the workshop. People in charge of the moderation will strive to entertain onsite and remote participation indiscriminately.

Proposed Additional Tools: Social media (Facebook, but not Twitter or Reddit, since they do not support IPv6) will also be employed by the online moderators who will be in charge of browsing social media using hashtag (to be defined).

SDGs:

GOAL 9: Industry, Innovation and Infrastructure

Background Paper

IGF 2019 WS #406 Ethical Hacking: Risk or chance for a more secure internet?

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Security Best Practice
Hacking
Security

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: Technical Community, Western European and Others Group (WEOG)
Organizer 3: Civil Society, Western European and Others Group (WEOG)

Speaker 1: Tim Philipp Schäfers, Civil Society, Western European and Others Group (WEOG)
Speaker 2: Sebastian Neef, Technical Community, Western European and Others Group (WEOG)
Speaker 3: Viktor Schlueter, Civil Society, Western European and Others Group (WEOG)
Speaker 4: Houston Sam, Private Sector, Western European and Others Group (WEOG)

Policy Question(s):

Within this workshop we want to address certain policy questions which are outlined here:
What is the status quo of ethical hacking and vulnerability reporting processes and how can it be improved?
Is ethical hacking viewed as an uncontrollable risk or a chance for a more secure internet?
What are the different stakeholder's interests?
How can responsible disclosure guidelines or bug bounty programs help to improve the internet's security?
What legal and ethical challenges arise in the context of ethical hacking?
How can those challenges be solved in the best interest of all stakeholders?
How should a best practice for vulnerability reporting look like?
Is it in all stakeholder intrests that there is a certain world-wide standard for vulnerability reporting (e.g. for government systems) and how can this be achieved?

Relevance to Theme: The security of IT systems or critical infrastructures are very important for a stable and reliable society. If those central systems are not working as intended prosperity, environments or lifes could be in danger.

The current development shows that there is a growing amount of connected devices and systems, therefore leading to a constantly expanding attack surface. Furthermore the professionality of cybercrime is constantly growing.
This means we not only need to adress the technial challenges, but also adapt an international, organisational standard for incident responses in order to ensure a secure internet.
One component could be allowing ethical hackers to conduct research and report security vulnerabilities to the providers or goverment agencies. Issues could be fixed before harm is done by a malicious attacker.
In the past there were several cases where ethical "white-hat" hacking lead to more secure IT systems and within the open-source community it is pretty common to report security risks to the maintaining party.
Several government Computer Emergency Response Teams (CERTs) have implemented a vulnerability reporting process in order to protect their own systems and the ones crucial for the well-being of the society - but there is no world-wide standard or agreement how to deal with ethical hacking, so most of the time this security research is acting in a "greyfield".

Furthermore, there are regulations in a few countries, e.g. the so called "IT-Sicherheitsgesetz" in Germany, which motivates providers of "critical infrastructures" to adhere to certain IT security standards. However, this is not enought because the internet is borderless, what makes security, safety, stability and resilience a global challenge.
Current political discussions focus mostly on prohibiting hacking or hacking tools instead of using the hackers' creative work in a positive way to build a more secure ecosystem. Right now, security researchers might face legal threats or repercussions. Several such cases (in which ethical hackers were criminalized) are known in the IT security community.

A positive side effect of allowing ethical hacking could be a constant (e.g. yearly) report about handled vulnerabilities or the state of the internet security. This could strengthen the trust in new technologies of the civil society, because they know that people care and think about their privacy and data on a global and not only national level.

Relevance to Internet Governance: The regulation and acceptance of ethical hacking can help to assure the security and stability of the internet. Security is only achievable when all participants of the global,

interconnected infrastructure - that we call the internet - work together. Due to it's distributed nature, it is not sufficient if only parts of the internet are secured, because they still can be attacked by unsecured and unpatched systems.
One way to assure the internet's stability is to convince policy makers that there is a need for certain standards of vulnerability reporting to facilitate reporting and addressing of potential security issues. Hacking in general should not be condemned but be seen as an opportunity to achieve higher security standards. A specialized framework and process that different stakeholders can rely on would immensely improve the current situation. The status quo does not provide any international standards on ethical hacking or guidelines on how to handle reports from security researchers. During the recent years the privacy aspect of internet governance developed in a quite positive way. For example most of the companies have a privacy policy and point of contact for issues in that regard. Having a similar point of contact for security related issues, especially for bigger organisations, is one of the goals. Internet Governance provides a multi-stakeholder way to discuss and implement the most pressing topics around "ethical hacking".

Format:

Break-out Group Discussions - Flexible Seating - 90 Min

Description: The workshop consists of multiple phases.

First, all stakeholders and a few participants get the chance to present their views in short introductionary statements and contributions to get a deeper understanding of the topics and current challenges. By exploring and discovering different common topics within the context of ethical hacking, all participants will gain an overview, common knowledge and different perspectives of the topic.

After that, the participants will be separated into topic-specific groups (e.g. legal challenges, ethical challenges, organisational challenges, etc). Each group will discuss one or more questions on their topic with the goal of trying to find possible and feasible solutions to them. All results and outcomes of the group work will then be discussed in the plenum by each group (presenters by 1-2 member each group).

The moderator will gather all results, take notes and close the working with an ending statement.

Possible timeline (~90 minutes):
- ~10 minutes x ~3 (~30 minutes): Introduction statement from diffrent stakeholder groups
- ~15 minutes: Discussion and exchange between the stakeholder views / view from different angles / looking for core topics and clusters
- ~20 minutes: Working on the core topics (for example: ethics, policy, legal, etc.)
- ~20 minutes: Getting together - presentation of the group work
- ~5 minutes: Conclusion / ending statement and next steps

Expected Outcomes: The result of the workshop should be that each stakeholder group knows about current challenges, the status quo of vulnerability handling and ethical hacking. We hope that we can facilitate a better understanding between the stakeholder groups and new impulses for developing a common standard routine for vulnerability disclosure processes.
As most security researcher worldwide still have to fear prosecution when disclosing vulnerabilities, common guidelines for vulnerability discosure processes could make the internet a safer place.

Discussion Facilitation:

The session will be interactive because we want to bring all important questions to the table. There is a lot of space for open statments and even people who don't want to present their ideas to a hugh audience could work on the topics they want to deal with in the smaller groups. Furthermore we will arrange an online moderator

Online Participation:

We want to use the remote participation for statements of security researchers worldwide.

SDGs:

GOAL 3: Good Health and Well-Being
GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 11: Sustainable Cities and Communities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #407 Social Media and Political Transition in The Gambia

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Civic Engagement online

Organizer 1: Civil Society, African Group
Organizer 2: Civil Society, African Group
Organizer 3: Government, Intergovernmental Organization

Speaker 1: Amadou SOWE, Government, Intergovernmental Organization
Speaker 2: Lamin Sanneh, Government, African Group
Speaker 3: ALIEU SOWE, Civil Society, African Group

Policy Question(s):

How Social Media is strengthening Democracy in The Gambia

Relevance to Theme: Social Media and Democratic Process in The Gambia

Relevance to Internet Governance: The Gambia is going through a transition process after 22 years of dictatorship. There is currently a new constitution being written. Social Media was a deciding factor in uprooting a dictatorship in The Gambia. The new government promised reforms but time and time again high profile officials make proclaimations calling social media as a threat to national security. There is less conversation from the authorities that is assuring about internet freedom in the new constitution . The New government came into power with a promise to stay in power only for 3 years and now the narratives towards that has dractivally changed. People are actually going to court for internet related crimes that the laws of the land do not cater for.

Format:
Break-out Group Discussions - Flexible Seating - 90 Min

Description: We will have speakers from various stakeholders groups in The Gambia to have an open discussions with contributions from the participants.

Expected Outcomes: Sharing and learning best practice with the audience
Rally international support to promote press and internet freedom in The Gambia and countries in democratic transition

Discussion Facilitation:

It will be an open discussion where participants will have the chance to share best practices.

Online Participation:

Usage of IGF Tool

SDGs:

GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #413 Human Values in Internet Protocols: What Can Be Done

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Democratic Values
Human Rights
Internet Protocols

Organizer 1: Civil Society, Western European and Others Group (WEOG)
Organizer 2: ,
Organizer 3: Technical Community, Western European and Others Group (WEOG)

Speaker 1: Farzaneh Badii, Civil Society, Asia-Pacific Group
Speaker 2: Avri Doria, ,
Speaker 3: cath corinne, Civil Society, Western European and Others Group (WEOG)
Speaker 4: Bradley Fidler, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

Human values and protocol design: What is the relationship between political values, such as human rights, and Internet protocols? Do certain Internet protocols have universal impacts on our politics, regardless of where they are used--or are the impacts of protocols on human rights more context dependent? What does the global history of the Internet teach us about the relationship between political values and Internet protocols? Insofar as protocols do impact our politics, is it possible to design protocols with explicit political commitments in mind? If so, what would the role of Internet organizations in this work? How would they maintain global support and legitimacy in such a practice?

Relevance to Theme: Security, safety, stability, and resilience are each features of the Internet that i) are consciously designed, ii) involve both technologies and organizations, and iii) respond to the needs of certain political values. Narrower technical definitions of these terms, which prevailed during the early years of the Internet, are giving way to broader, societal definitions that involve both technology and the social orders with which it intersects. To pursue any of these goals, then, we should be clear about the extent to which their societal components can be furthered with technical design, and the extent to which they cannot.

Relevance to Internet Governance: Internet Governance deals not only with technical standards but with "shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." The globalization of Internet governance has not simply expanded the Internet: its globalization has also brought the world's political values to bear on the Internet's design. Historically, Internet protocols have often been assumed to further some variant of American values--a claim made explicitly in the US National Cyber Strategy--although developments of the last decade or more have demonstrated, instead, the that Internet can support multiple, and even conflicting, political values. Today, the question is how the Internet can be made to support which political values, through a combination of governance, administration, and redesign. Our debate will be on the possibilities of redesign, what

opportunities it can provide, and what it means for the future of the Internet and Internet Governance.
This proposed debate will be about the extent to which principles, norms, and rules can be furthered through technological design. Already, this topic has been pursued as a research and policy agenda through the Human Rights Protocol Considerations (HRPC) Working Group at the Internet Research Task Force (IRTF) (initially through the work of Corinne Cath, a participant in this proposed debate, among others). We hope to broaden this discussion of the relationship between political values and Internet protocols beyond the IRTF and its peer organization the Internet Engineering Task Force (IETF), and make it a global topic of discussion. This discussion is already underway in governments, activist groups, academia, and private firms: we hope to make it explicit, and global, at the IGF.
This debate is not about which political values we should attempt to further through technological design. Rather, it is about the conditions and possibilities for doing so, questions that intersect both research and policy: i) what do we know about the relationship between values and protocols, ii) what can this knowledge accomplish, and iii) what should we do about it? The first point, our knowledge about the relationship between values and protocols, is important because it is the basis for any positive program of change. Are there strong historical precedents for a protocol furthering a specific set of political values? Without such a precedent, can there be a program? Already, debate is forming over the history of protocols and how they can inform present-day action. The second point concerns what we might be able to accomplish with this information. If some Internet protocols have demonstrated an ability to further specific political values, then is it possible to design protocols with future political objectives in mind--or are we limited to retrospective analysis? Finally, the third point concerns the role for such activity in Internet Governance today. Purely technical organizations appear to lack the global legitimacy that would be required to push political programs through technical design: which organizations would be up to the task? Would they require different, or broader, mandates?
Ultimately, should the practice of Internet Governance include the explicit political considerations of protocol design?

Format:

Debate - Auditorium - 90 Min

Description: This debate is structured around the following question: given that Internet protocols have political implications, should prospective political implications be institutionalized as part of protocol development by standards bodies? This question requires a stance on the three issues above: what lessons we have learned from the past, what those lessons tell us about what is possible today, and the resultant potential roles for Internet Governance organizations. The objective of the debate is to alter the audience opinion from the original baseline (as detailed below).

Our session begins with an introduction by the moderator, and a concise, ten minute presentation by each speaker on their position on the issue. Broadly speaking, two confirmed participants support these political considerations, and two oppose them. Following these statements, the moderators will poll the in-person and online audience and determine the ratio of support for each position, and inform the audience that the objective of this debate -- through the work of the speakers and the audience -- is to shift opinion, which will be measured again at the end of the session. This will allow us to evaluate the course of the debate, and increase audience buy-in.

Next, each speaker will be provided with five minutes each to respond to the other speaker's opening statements. Following this, the moderators will structure a mix of online and offline discussion, with comments or questions (so long as they are directed at a speaker) limited to one minute per audience participant comment (multiple but not limitless comments will be allowed from individual audience members). At the conclusion of the session, a new poll of audience opinion will be taken and the outcome of the debate summarized by the moderator: the benefits and trade-offs of each position.

Expected Outcomes: We want to use debate to focus a diverse community on the opportunities and challenges that lie in attempts to further political goals through technical design. This includes, mainly, if such activities are possible and reliable, and if so, how might they be institutionalized in the Internet Governance community.

Discussion Facilitation:

Prior to and during the session we will use social media (as well as traditional platforms, such as listservs) to post information about the debate. We will draw on our media contacts to draw attention to this new format, and experiment with drawing in more public participation at the promise of a lively debate.

Online Participation:

In advance of the session, we will publicize this tool and encourage participation. Due to the novel kind of panel, we are optimistic that we can drive online participation in ways that would not be possible with a typical panel.

Proposed Additional Tools: Our online moderator will draw in participation from Twitter and Mastodon. We are investigating the possibility of attempting similar on Weibo.

SDGs:

GOAL 4: Quality Education
GOAL 5: Gender Equality
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions

IGF 2019 WS #416 Popular Movements for Peace in Cyberspace

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Civic Engagement online
Cyber Attacks
Human Rights

Organizer 1: Private Sector, Western European and Others Group (WEOG)
Organizer 2: Private Sector, Western European and Others Group (WEOG)
Organizer 3: Private Sector, Eastern European Group

Speaker 1: Jamal Edwards, Private Sector, Western European and Others Group (WEOG)
Speaker 2: Deborah Brown, Civil Society, Western European and Others Group (WEOG)
Speaker 3: Ephraim Percy Kenyanito, Civil Society, African Group

Policy Question(s):

What can we expect from the next generation of leaders working to bring about peace in cyberspace?
What does cooperation and digital inclusion look like for young people in the online world?
What can we learn from the global initiatives rising around the world advocating for a more peaceful and trusted digital domain?

Relevance to Theme: Amidst the current atmosphere of escalating tensions between nations in cyberspace, resulting in the development of increasingly sophisticated cyberweapons, it is more important than ever that young people, digital natives, etc. step up to demand more from governments, and all stakeholders in the digital ecosystem. The economic and social benefits brought by increased peaceful activity in cyberspace are at risk in the face of an arms race between competing nation states that threatens to envelop innocent users, critical infrastructure and other private entities as collateral damage. The next generation of leaders must not only be listened to but also be provided a platform to speak. Cyber security, trust, and resiliency will

not happen on its own, it must be fought for—especially in emerging economies. This is why the current global initiatives this panel will highlight are so key to further discuss and to also identify areas where more needs to be done.

Relevance to Internet Governance: The challenge addressed in this proposed session is how to proactively and intentionally coordinate actions—especially amongst young people—to create peace and movements that build trust between nations, communities. This discussion cuts to the core of a number of internet governance challenges and inherently requires engagement by a range of stakeholders to explore how such efforts to bring peace should be designed and inspired – based on established norms and expectations – to protect a safe and secure internet.

Format:

Panel - Auditorium - 60 Min

Description: Governments are increasingly attempting to exploit or even weaponize software to achieve national security objectives, and governmental investments in military cyber capabilities continue to grow year after year – civilians and emerging economies are a frequent collateral of this escalating cyberconflict. This panel will highlight a new generation of collaboration among people from around the world, coming together to fight for their right to a free and secure internet. Panelists will discuss key new and inclusive initiatives – including the Digital Peace Now campaign, Paris Call for Trust & Security in Cyberspace and Tim Berners-Lee's Contract for the Web – and also explore what the next steps might be for this growing movement. The session format will allow speakers to present their respective points of view as it relates to ongoing movements and efforts on the horizon, as well as the opportunity to challenge and respond to one another on which approaches might be most effective. Importantly, the session will help educate those attending the session on this emerging area of peace movements and leave ample time for questions directly from those in attendance to the panelists.
Agenda:
• 5 minutes – Opening remarks from moderator setting the stage for the discussion, highlighting the current state of affairs.
• 10 minutes – Opening remarks from panelists sharing their perspectives on the major peace movements in the last year, how they differ, and detail a new generation of digital inclusion.
• 30 minutes – Moderator asks pointed questions to respective speakers about avenues for advancement in this space and highlighting where there seem to be obstacles to further progress. Speakers will respond both to direct questions as well as to one another, representing both their individual and stakeholder perspectives as it relates to the positions of others. This portion of the session will identify points of agreement and divergence for those in attendance.
• 15 minutes – Those attending the session, in the room or remotely, will be welcomed to ask direct questions of the speakers and share divergent perspectives. Once again, speakers will be encouraged to both address the questions that are asked as well as to respond to the answers provided by their colleagues.

Expected Outcomes: This session will provide important learnings and highlight significant opportunities for those in attendance from all stakeholder groups seeking to find ways to support the growing international movements for peace in cyberspace through meaningful actions to promote inclusion and multistakeholderism. For representatives from nations still establishing a posture on these issues, this session will highlight the various initiatives and opportunities for stakeholders across the digital ecosystem and especially young people to engage and advance their interests and build relationships in this space.

Discussion Facilitation:

Please see part B.

Online Participation:

The Q&A portion of the session will engage online participants and will explicitly solicit requests for input, questions, and feedback via the online participation tool. This is a key part of the agenda following the

panelists opening remarks and shared perspectives on global peace initiatives and efforts for cyberspace.

SDGs:

GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals

IGF 2019 WS #417 Online Gender Violence: Actions and reactions from feminist

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Online gender violence

Organizer 1: ,
Organizer 2: Civil Society, Latin American and Caribbean Group (GRULAC)

Speaker 1: Janara Kalline Leal Lopes de Sousa, Civil Society, Latin American and Caribbean Group (GRULAC)
Speaker 2: Patricia Pena Patricia Pena, ,
Speaker 3: Lourdes Barrera, Civil Society, Latin American and Caribbean Group (GRULAC)

Policy Question(s):

What have been the lessons learned from the different actions, initiatives and strategies of feminist women's organizations and groups to face online violence against women?
What have been successful cases of advocacy for public policies on gender-based violence online and what can we learn from it?
What have been the most appropriate ways to achieve an impact on public opinion, generate advocacy and achieve changes in political, judicial and administrative systems that incorporate gender perspectives that allow for addressing gender-based violence online?

Relevance to Theme: The proposed workshop is relevant because online gender violence is a current issue, however, it is an issue that has been subject of studies, advocacy campaigns, digital measures, toolkits, and other different responses. All these have in common that are responses from a gender perspective which have been the reason many times of their success.
It is precisely from these experiences that the Workshop will try through various representatives of organizations to generate activities that reveal where are the weak points in strategic, where are the complex situations to provide support to victims, and how has been possible to achieve success in actions and reactions against online gender violence.

Relevance to Internet Governance: Along of the years we can see that the important changes starts from a crisis which now is visualize it -thanks to the technology - faster and clear, on many ways. Now, with the point of view of the feminism and its actors the idea is to contribute and to solve the issue together with the the representative of other sectors to improve the measures and helping the victims in the best way possible.
Today the issue is on the table, and we cannot ignore the thousands of victims of gender violence around the world. This violence which tends to be more and more aggressive, but so far there is not an effective tool which can take away the danger of that , so it is time to find a way together to make the difference, learning from our mistakes and find better ways to combat this.

Format:
Round Table - Circle - 60 Min

Description: Our session will consist to show to attendees and participants the differents tools which have been use to combat and aware the online violence based on gender during the last year such as media campaings, strategic litigation, IA, etc.
Every panelist will have 8 minutes to explain their tools and how this has been effective or not in their environment.
For example Acoso Online will explain their research regarding online gender violence, highlighting the opportunities and challenges of the research.
Our intention is to develop a session to articulate collective strategies, plan campaigns and other actions among several NGOs and working together with the rest of the representatives to discover which tools are the more effective ones.
To conclude, there will be an open space to the audience to make questions and comments about it, because our most important concern is to know from the attendees -in their own opinion- which the presented tools, seems to be more effective and what are the weaks points of each of them, with the compromise to work on improve them and even change our point to address the issue.

Expected Outcomes: The format of the session, presentation first and group comments after, seeks to receive how the discussion follow, and collect the reactions and ideas, in order to develop strategies collectively, from Academia, Companies and pairs.

Discussion Facilitation:

We will provide to audience at the begining of the workshop a a list which includes every ways to gender violence which can find online and we ask them which the presented tools they find more effective one against each situation.

Online Participation:

Using twitter with hashtags to comments the workshop in order to find online question that could response at the end of the session.

Proposed Additional Tools: Twitter with the useful hashtag to the workshop.

SDGs:

GOAL 5: Gender Equality
GOAL 10: Reduced Inequalities
GOAL 17: Partnerships for the Goals

IGF 2019 WS #420 Digital Security at the Grassroots: Emerging needs and chall

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Anonymity
Human Rights
Security

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, Asia-Pacific Group

Speaker 1: Datta Bishakha, Civil Society, Asia-Pacific Group
Speaker 2: valentina pellizzer, Civil Society, Eastern European Group
Speaker 3: Gilberto Cutrupi, Civil Society, Western European and Others Group (WEOG)

Policy Question(s):

What role should different stakeholders play in cybersecurity capacity building approaches?
What role can the implementation of the principles of safety by design, privacy by design and by default as a principle play to secure human rights and achieve increased safety?

Relevance to Theme: This session foregrounds the experience of addressing digital security in grassroots communities in Asia, and is based on their lived realities, holistic security needs, and technical challenges. It aims to push the conversation on technology-enabled violence and digital security beyond online violence, and look at ways to address threats which are digital but not necessarily online.

Out of the 5.1 billion mobile phone users in the world, an estimated 2.5-3 billion are smartphone users. The difference is much wider in global south economies like India where three out of four mobile phone users use a basic phone. The conventional digital security curricula does not address the violence faced by the basic mobile phone users, a lot of whom are teenagers, women, trans and queer persons who cannot afford smart phones.

However, like everyone else who uses digital devices, women and young people in these grassroots communities are aware of the need for digital security - security that is holistic, based on their lived realities and tailored to the digital devices they use.
This session aims to bring in pertinent issues which are of relevance in developing countries in relation to security, safety, stability and resilience, taking into account a multidisciplinary perspective which includes diverse stakeholders who will otherwise be left out of this dialogue.

Relevance to Internet Governance: This session contributes to the mandate of broadening and including issues related to technology and internet governance that are of relevance in global south economies. It is essential for digital security to address the needs of all users, and not just of those working in technology or digital rights, or those with access to more advanced technologies.
For internet governance and internet governance spaces to be truly inclusive of all users of digital technology, and to work towards increasing access and space for those who are not from a privileged country, class, gender, sexuality, religion, ability, or caste, this session under the theme of security, safety, stability, and resilience will be an important step. It will allow us to reflect on who is missing and why, and what do we need to do next. Moreover, without feeding this knowledge into internet governance discussion and spaces, we will not be able to develop better governance principles and mechanisms that are internationally valid. This global regulatory action is one of the things which can improve our internet experiences, as said by Vint Cerf.

Format:
Round Table - Circle - 90 Min

Description: What do we talk about when we talk about digital security and safety? And what do we not talk about when we talk about digital security and safety?
Conversations on technology-enabled violence and digital security tends to be about online violence, or violence on the internet, including but not limited to verbal abuse, rape threats, non-consensual sharing of images etc. Another part which is thought and talked about much less is violence which goes beyond online to digital. That which may not be online but is digital.
One of the first steps one takes to protect their device, a mobile phone or the computer, is to use a password to lock the device. But what if you're a 19 year old college student living with her parents in India and they ask you unlock your phone? What if you are woman who has no choice but to share your password with a family member, husband or partner? How do rural journalists who are harassed by incessant phone calls from strange men protect themselves? What do trans persons who receive demands of sex on social media do to address this? What are some digital security threats faced by LGBTQI persons in countries which have homophobic and transphobic legislations and norms?

These are some of the questions which we will be discussing and trying to answer during this session. Without taking digital security to the grassroots, and meeting them where they are, the purview of current

digital security curricula will leave out a large demographic, focussing only on part of the problem.
This session will be in the form of a panel discussion with speakers working on digital security with diverse demographics presenting their challenges and learnings from this work. The main aim of this session is knowledge-sharing which will help bring together digital security, usability, and grassroot users. One of the speakers will also be a digital security trainer who will input from a technical perspective, which will help in closing the gap between digital security requirements and existing knowledge.

Expected Outcomes: This session will have speakers from different regions working on a range of issues who will be sharing their work around ensuring digital rights, human rights, and privacy at the grassroot level. Best practices which can be adapted and implemented in other spaces will be pulled out and collated. This will be a direct capacity building outcome. This session will also actively contribute to increasing diversity of participants as well as of conversations around digital security, technology-enabled violence, privacy, and safety.

Discussion Facilitation:

There will be a question and answer, and input round after the speakers present. A mic will be passed around in the room for taking inputs and questions from the onsite participants. Smita Vanniyar will be reading out the questions and inputs from the remote participants to the whole room so that they are a part of the discussion and not isolated from it.

Online Participation:

We are planning to have at least one speaker who will be joining in remotely. The Official Online Participation tool will be very beneficial in this process. Apart from this, we want to use this tool to increase engagement with others working on similar issues who may not be present onsite at the IGF as this will directly contribute to the outcome of the session which is knowledge sharing.

Proposed Additional Tools: We will be live tweeting the whole session to ensure that the conversation does not just stay inside the room, or just at the IGF. This will also include provisions to take questions from the online participants via social media as well as from those participating remotely on the IGF platform.
We will also set up a Sli.do page which will be promoted before and during the session to allow for more continuous inputs and questions from the participants, both onsite and remote.

SDGs:

GOAL 5: Gender Equality

IGF 2019 WS #423 SOCIAL ENGINEERING: Most Recurrent but Neglected Cybercrime

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Cyber Attacks
Hacking
Security

Organizer 1: Civil Society, African Group
Organizer 2: Technical Community, African Group
Organizer 3: Civil Society, African Group

Speaker 1: Samuel Osei Mensah, Civil Society, African Group
Speaker 2: Lily Edinam Botsyoe, Technical Community, African Group

Speaker 3: Gabriel Karsan, Civil Society, African Group

Policy Question(s):

What is Social Engineering?
How it is impacting the digital society?
What are Social engineering attack techniques?
Best Social engineering prevention methods

Relevance to Theme: Understand the concept of social engineering
Learn what makes social engineering especially dangerous
Learn about social engineering attack techniques
Understand social engineering prevention

Relevance to Internet Governance: Today, the Internet is the most powerful tool in the world and has undoubtedly become an important element in our life. Individuals, organizations and governments are relying on the internet for a lot of activities including sharing sensitive information. However, like every single innovation in science and technology, the internet has its own advantages and disadvantages. Social engineering attacks happen in one or more steps. A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. The session is part of safeguarding the Internet against the manipulation of human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps.

Format:
Round Table - Circle - 60 Min

Description: The risk of disclosure of sensitive information constitute the major disadvantages of using the Internet and as it is continuing to evolve, organizations and governments have a vested interest in securing sensitive information stored or shared over the internet. Theis session is to address and draw attention to the protection of sensitive information and the development of countermeasures against illegal access to information are of vital importance to organizations and governments to ensure the trust of clients and citizens. The session will discuss all issues around Social Engineering and it will take a round table discussion.

Expected Outcomes: Organizations and governments have been spending hundreds of thousands of dollars investing in firewalls, intrusion detection systems, encryption systems and other security technologies to prevent cyber criminals from having access to their sensitive information. The session will highlight on latest trends and new preventive ways of using the web.

Discussion Facilitation:

There will be open questions to keep participation going while organizers will engage other experts to talk on topic for better dialogue.

Online Participation:

Through social media awareness of the topic prior and during the session organizers plan to include all person available/joined online slots to contribute their questions, suggestions and experience on the topic.

Proposed Additional Tools: Organizers plan to utilize the emerging growth of Youth from Africa interested in keeping the internet healthy. These youth are mostly on major social media platforms: facebook, Twitter and Instagram. In the form of Twitter Chat and updates, we hope to engage more to increase participation.

SDGs:

GOAL 4: Quality Education
GOAL 5: Gender Equality

GOAL 8: Decent Work and Economic Growth
GOAL 9: Industry, Innovation and Infrastructure
GOAL 10: Reduced Inequalities

Background Paper

Reference Document

IGF 2019 WS #430 Dual-use Technology Export:Threats to HR and Freedom

Theme:
Security, Safety, Stability and Resilience

Subtheme(s):
Democratic Values
Resilience
Security

Organizer 1: Civil Society, Asia-Pacific Group
Organizer 2: Civil Society, African Group

Speaker 1: Khalid Ibrahim, Civil Society, Asia-Pacific Group
Speaker 2: Nardine Alnemr, Civil Society, African Group
Speaker 3: Wafa Ben-Hassine, Civil Society, African Group

Policy Question(s):

Surveillance and violation of privacy have been the central human rights concerns in advocacy for a dual use technology export ban. Evidence from cases across the Gulf and neighbouring countries demonstrates that they are far more risks in the absence of export ban. Therefore, the policy questions we aim to address in this session are:
1) To what extent do surveillance tools affect the physical security of targeted human rights defenders including online activists and bloggers?
2) What are the implications of mass surveillance tools on the resilience of human rights activism and the whole human rights movement in the Middle-East?
3) How would a dual technology export contribute to stability in human rights activism and advocacy?

Relevance to Theme: Dual use technology have a duality pertaining each item of the theme. The technology have been imported by governments in the Gulf countries as part and piece of their political stability and security claims. As they are developing a cybersecurity and cybercrimes paradigm which heavily penalises and criminalises human rights and freedoms, their claims are questionable. Therefore, we look at security at both ends: the claims of national security through the use of surveillance technologies, and human security of arbitrarily targeted human rights defenders. For stability, it is stability of oppressive governments versus stability of human rights activism and advocacy, and similarly the resilience of a crackdown on digital rights vis-à-vis resilient civic space for exercising human rights and freedoms. In this discussion, we have a particular focus on conflict-torn communities as in Yemen and Syria where the duality of security, safety, stability and resilience are intensified.

Relevance to Internet Governance: Agreeing that internet governance should be guided by the Universal Declaration for Human Rights and UN Human Rights Conventions, we are driven to institutionalise the respect of freedoms of opinion, thought, expression, and right to privacy in the governance of technologies. The development of a dual use technology export ban requires the collective efforts of different stakeholders. Essentially, governments and international governmental organisations should be engaged in

the formulation, enactment and holding governments accountable for the mandates of an export ban. In addition, with collaboration with the private sector and tech community, the export ban can be introduced through the lens of business and human rights. This lens encourages private companies and the tech community to be aware of the consequences of practices that perpetuate human rights abuses. Therefore, not only the export ban requires collective effort to develop it but also to enforce it and keep checks, a task mainly for civil society but also should be introduced to governments, IGOs and the private sector.

Format:

Round Table - U-shape - 90 Min

Description: Security and stability are important internet governance issues in the Middle East and North Africa. Developing a solid cybersecurity and cybcercrime legislation, supported with cyber security technologies has been the means to ensure security and stability. However, because security and stability in this context is only concerned with the politics of governments in the region, it has rarely catered for the security and stability of most stakeholders. In importing dual use technology, the Gulf and neighbouring countries have enforced oppressive cybersecurity and cybercrime laws which penalize and criminalize freedom and human rights. In this session, we examine the implications of dual use technology on human rights and freedoms. Especially, the duality it exhibits of governments security versus human security, resilient oppression versus resilient human rights activism, and stable coercion in contrast with unstable civic space.

Expected Outcomes: We expect this session to have two outcomes: informative and active.
The informative outcomes is interactive, meaning that panelist are informing audience on their findings and remarks on possible governance solutions while also learning from audience.
The active outcome is two-faceted. First, introducing audience to the different efforts of stakeholders represented by each panelist in attempt of opening avenues for collaboration and networking. Second, by crafting actions that support previous advocacy that aimed to enforce a dual use technology export ban.

Discussion Facilitation:

We are there to keep the discussion flowing and focused, and to ensure all participants have an opportunity to contribute. Various professionals don't often get the chance to meet others in their field so this is a unique opportunity to meet other attendees during our round table session which will allow attendees to thoroughly explore an issue with the aid of a knowledgeable, experienced moderators and speakers.

Online Participation:

We will use the full potential of the official online participation tool. In addition we are going to use our active accounts on social media networks to encourage participation.

Proposed Additional Tools: A special flyer will be designed for the session to encourage people to attend the session in person and equally we hope to live-stream the session on our various online accounts in order to increase online participation.

SDGs:

GOAL 10: Reduced Inequalities
GOAL 16: Peace, Justice and Strong Institutions
GOAL 17: Partnerships for the Goals