IGF-2016 Report on Workshop # 143

Session Title
How to Acknowledge Cyber Evidence: Reform or New Parallel Law

Date
December 7, 2016 (Wednesday)

Time
0900 – 1030 Hours (Workshop Room # 5)

Session Organizer
Khan Muhammad Fuad Bin Enayet

Chair/Moderator
Dr. Walid Al-Saqaf

Remote Moderator
Izumi Okutani

Rapporteur/Notetaker
Khan Muhammad Fuad Bin Enayet [by Remote Participation]

List of Speakers and their Institutional Affiliations

1. Mr. Sumon Ahmed Sabir
   Chief Technology Officer (CTO), Fiber@Home Limited
   Policy SIG Co-Chair, APNIC
   Chairman, Board of Trustee, bdNOG

2. Mr. Babu Ram Aryal [by Remote Participation]
   Chairman, Center for Law and Technology Pvt. Ltd.
   President, Forum for Digital Equality
   Internet Lawyer and Consultant, Nepal

3. Mr. Andrew Doymana
   Director for Information Technology at the Ministry of MEIDECC
   Government of Tonga

Key Issues Raised (1 sentence per issue):

1. How to address and acknowledge the cyber evidence where virtual and real life activities should be treated equally with logical consequences of happenings and identity confirmation. And so that means that how to deal with virtual and real world when it comes to evidence.

2. Whether the modernization and/or amendment of classical criminal procedure, evidence law, etc. are good enough to manage the Human Rights and criminal activities in Internet domain. That is to discuss about the coexistence of real and virtual domain.

3. Whether the law enforcement activities, for example, surveillance, intelligence, policing, defence, etc. are going to require separate legal and administrative frameworks. What we need, documents / frameworks drafted from scratch to separate the real and virtual domain for the sustainable ecosystem.

4. Short and long term governance model for the Internet, legislature and Internet ecosystem.

Summary on Presentation (1 Paragraph)

No separate Presentation were made in the workshop

Discussions that took place during the Workshop (3 Paragraph)

There are different kind of criminal activities. The criminal activities is a criminal activity, which is also available in real time. So, if we consider the crime only and the respective evidence to judge the outcome of that crime, we will always find that there's a remedy in traditional law. So, for every kind of medium and evidence we should not go to have a new law. Our focus should be to incorporate the acceptance of new kind of evidences e.g. cyber evidence in activity-log, sms, e-mail etc. Beacause it's not practical to update a law in every year. Moreover, Cyber Law could be used as an oppressive tool to the political opposition.

Cyber Crime doesn't have any boundary and to have cross-border support from the counterparts, a legal framework is very much needed. Court of Law requires specific legal proceedings, evidence presentation and as it has cross-border nature there is a need of international administrative procedures. Hence, Laws should be written in a way that it lasts for long, particularly for cyber / ICT laws. Cyber law shall ensure the acceptance of cyber evidence. We need to incorporate the procedures like: collection, preservation and presentation in front of court, but, it should not be very technical so that it needs to be replaced within years.

Right now, real-life crimes are prosecuted with cyber evidences starting from simple wrong-parking to kidnapping / killing. But considering a cyber-crime with evidence is the challenge. But in places, cyber law is being abused against the freedom of speech, blogging, etc. As, the internet / cyber activity is beyond political borders and truly international by nature. We may need to have an International Standard Treaty to mitigate those problems. But, that should be an umbrella alike model not very deep in technical details, neither dealing with every single crime. We may need something alike of Budapest Convention for Cyber Evidence and associated issues.

Cardinal Suggestions / Key Takeaways from the Workshop (3 Paragraph)

There were very sporting debate regarding the need of cyber law. Majority of the speakers are in opinion that we should have some form of cyber law. However, there was also agreement that it need to not take things to the extremes, to the details, to the level that makes cyber law not possible to implement. Therefore, one thing to ensure that there is something, some baseline, some commonalities, common ground that everyone can agree with, which would foster international collaboration and fighting Cybercrime. But on the other hand, some countries may take it to the extreme either too technically by elaborating on things, making laws very difficult to make laws to continue to evolve and sometimes to sue protocol east citizens to suppress dissent. And in some cases cause more harm than good. But if you think of in terms of the benefit of society at large, the benefit of citizens, keeping them safer, then having some sort of guidance there that's uniform, that's standard, that's based on digital evidence, good practices is very useful and it can be elaborated more and clarified in ways that help society at large.

However, there was something that Moderator felt was a bit missing in this discussion, which was the competence of the law enforcements agencies, evidence collectors, judiciary systems, judges, juries and everyone, complete understanding what is going on in the Internet and cyber world. Authenticity of evidence is something really to do in top-notch manner. This has been mentioned in different workshops, in different events. And that's why there were capacity building programmes for individuals from lawyers, to judges, to civil servants, to police forces to understand how the Internet is shaping our world and making us a need for these competences and abilities.

We may need to have an International Standard Treaty to mitigate those problems. But, that should be an umbrella alike model not very deep in technical details, neither dealing with every single crime. We may need something alike of Budapest Convention for Cyber Evidence and associated issues. The ideas that have been floating around are very much ingrained bodes as citizens and governments and law enforcement units as well as technologists and lawyers. But on the other hand, it's still promising that we have a way to debate this openly, fairly in a sense of sportsmanship and spirit of understanding that we can disagree but eventually it's the interests of the end user that matters.

IGF's Gender Reporting

1. Estimate the overall number of the participants present at the session
   20 Persons

2. Estimate the overall number of women present at the session
   8 Persons

3. To what extent did the session discuss gender equality and/or women's empowerment?
   The topic was about Cyber Evidence and Legal Procedures in Virtual World. The gender equality and/or women's empowerment was not discussed in the workshop

4. If the session addressed issues related to gender equality and/or women's empowerment, please provide a brief summary of the discussion
   Not Applicable