IGF 2016 session DC IoT

Session Format

Panel and interactive session with participants

Duration

90 minutes

IGF 2016 subtheme

Dynamic Coalitions

Description

The IGF Dynamic Coalition on the Internet of Things (IoT) brings together stakeholders from all over the world to engage in a dialogue on "good practice" in IoT, with the intent to find a realistic and long term sustainable way forward.

Since the 3rd Internet Governance Forum (IGF) meeting in Hyderabad (2008), IoT has been on the agenda for multi-stakeholder discussions of all IGFs, and the Dynamic Coalition on IoT continues to raise attention for the potential as well as challenges of the emergence of a world in which increasing proliferation of sensors and actuators connected to the Internet, which collect, act and share data, both among other things and with people.

The Internet of Things is still in early stages, and in many ways new possibilities are developed and discovered beyond our imagination, and we welcome it for its potential to help alleviate specific societal challenges where it can. The Internet of Things has, however, been around long enough to already a history with consequence. Following the DC meeting during the IGF in Istanbul in 2014 and subsequent meetings during 2015, we came to the conclusion that in order to foster both innovation and user trust in the Internet of Things, like the Internet, a careful balance should be struck between regulation and innovation. In 2015, this lead to the publication of a draft document on Global IoT Good Practice that was shared on the IGF platform and subject of discussion during the DC IoT meeting during the IGF in Joao Pessoa.

We came to understand that the way forward is to be found in taking ethical considerations into account from the outset, both in the development, deployment and use phases of the life cycle, thus to find a sustainable way ahead using IoT helping to create a free, secure and rights enabling environment.

In addition, in 2016 we witnessed the first large-scale use of IoT objects vulnerabilities as IoT devices are now deployed for massive DDOS attacks. Responsibility for ensuring abuse of devices for such action should be attributed thus to ensure action will be taken to counter such abuse towards the future.

Following the IGF meeting, taking into account feedback on the IGF online platform and having discussed this face to face during meetings in Brussels (EuroDIG, 8 June 2016) and Washington DC (USA IGF, 14 July 2016), an updated paper is presented at:

<WEB ADDRESS – BY PREFERENCE IGF PLATFORM OTHERWISE @ http://www.iot-dynamic-coalition.org/)

This declaration is on the table for this session. During the session, and over the coming year we want to further zoom in to what "good" looks like from a global multistakeholder perspective, and how sustainable development of IoT that is trusted, useable, accessible, affordable and profitable (in societal and/or business sense) can take place

Name, stakeholder group, and organizational affiliation of co-organizer(s)

Many people from different sectors and around the world have contributed over the years to the work of the Dynamic Coalition. Coordination of the work is currently in the hands of Wolfgang Kleinwaechter (one of the founding members), Avri Doria, Sandra Hofenrichter, Dan Caprio and Maarten Botterman (current Chairman of the DC).

The link to the work of the DC

Reference to the DC's earlier work can be found on the DC IoT website at http://www.iot-dynamic-coalition.org/.

Subject matter #tags that describe the session

#iot; #ethical_iot; #internetofthings; #internetofeverything; #industrial_internet; #privacy; #ethics; #bigdata; #sustainable; #humanrights

Description of the plan to facilitate discussion amongst speakers, audience members and remote participants

The DC workshop will be orientated around 5 key ideas that are reflecting our current thinking working towards a common appreciation of IoT good practice in 2016. These ideas are at the core of the draft declaration on IoT best practice that has been published on the IGF website. The ideas on which we would like to receive feedback are:

1. Defining "Ethical IoT": *Explaining "ethical" in IoT perspective requires a multistakeholder dialogue: In terms of "ethical" it was remarked that a proposed "ethical approach" should find a balance in being "sufficient" from a civil society point of view, and "do-able" from a business point of view, and sustainable from a technical point of view, in the end leading to a balance of trust and "profitability" (in societal and/or business sense) that fosters a fertile environment for further development of connected technologies and services including those that make it possible to tackle societal challenges that could not be tackled, before.*
2. IoT to address societal challenges: *Overall, IoT was seen as "coming" and "promising" and necessary to be able to address specific societal challenges. In this it is important to ensure developing countries can and will benefit from IoT applications as well, such as in agriculture and disaster warning systems. Possibly a "Principle" on "using the most available technology possible" so that for instance GSM networks can already facilitate creation of and interaction with IoT ecosystems in developing countries. Aim is to develop an annex to the declaration with examples of good practice in a variety of applications.*
3. Global Ontology for IoT: *IoT is not one big animal: it is an ecosystem with many elements. It is important to distinguish the specific IoT application, before becoming more specific than "generic". We need to develop an ontology for IoT applications with respect to: a. Privacy sensitivity; b. Security level required, not only for protecting data but also for avoiding*

      unauthorized tampering; c. Safety level required, much depending on the type of application and sector.

4. Awareness raising: *Need for IoT awareness with citizens and consumers: In terms of "making people aware" it was pointed out that "meaningful transparency" also means that people should not be expected to be technical experts.*
    a. *One way of dealing with this is using simplified codes (like the washing labels on clothing), and clear language reference sites, like a "Wikipedia for IoT", where possible;*
    b. *Another important factor is for users to have choice and ownership, and where this is not possible, for business to commit to "fairness" –a concept to be further developed over the coming year;*
    c. *The third element is the "expertise" element: how can we ensure independent trusted expertise is available to explore further whether systems are doing what they promise - possibly to be guaranteed by governments.*
5. *Securing the IoT infrastructure has two aspects that need to be addressed:*
    a. *IoT devices are inherently vulnerable themselves, as both sensors and actuators may be compromised via hacks and cyber attacks. Depending on the IoT application, appropriate measures will need to be taken that are proportional to the security and/or safety challenge;*
    b. *IoT devices are often connected to the Internet and, when not well protected, can be "recruited" to become part of increasingly massive size botnets that can be used for DDOS attacks. Proper security avoiding easy capture is therefore also a necessity. This will need to come with appropriate attribution of responsibility in ensuring this to be the case.*

Names and affiliations (stakeholder group, organization) of the participants in the session

Participants of the open Dynamic Coalition for IoT, which is open to all of the Tunis Agenda defined stakeholder groups

Name of in-person Moderator(s)

Avri Doria

Name of Remote Moderator(s)

Sandra Hoferichter

Name of Rapporteur(s)

Maarten Botterman

Description of the organizer's plans for remote participation

The DC IoT declaration is on line and open for comments. All comments prior to the day of the workshop will be considered by the Chair of the DC and will be reflected as much as possible in his opening statement to the meeting, when introducing the draft declaration.

In addition, the ideas underlying the draft declaration will have been presented on-line (as well as physically in the IGF conference facility) to the community, and feedback is welcome on that, too – via the facilities offered by the IGF secretariat.

When streaming of the session is available, questions will be taken via the remote moderator to the session.

Background paper

The draft declaration can be found on the DC IoT website at http://www.iot-dynamic-coalition.org/.

Agenda

1. Opening, introduction of the why and what of the draft declaration on IoT Best Practices by Maarten Botterman, Chairman DC IoT (10 min.)
2. Background to the draft declaration: history and thoughts on ways forward by Wolfgang Kleinwaechter, University of Arhus, ICANN Board (technical community) (10 min.)
3. Panel, moderated, with representatives from all sectors preparing short statements as "committed contributors" to this session (30 min.)
   Confirmed "committed contributors" include:
   1. Karen Rose (Information Society) confirmed
   2. Olga Cavelli (ITU WS20)
   3. Jari Arkko (Ericcson, Chair IETF)
   4. Megan Richards (European Commission)
   5. Grace Abuhamed (NTIA)
   6. Joseph Alhadef (ORACLE, Chair ICC BASIS)
   7. Max Senges (Google)
   8. Virat Bhatia (AT&T)

4. Open discussion with all participants and panel), moderated (40 min.)