Dynamic Coalition on the Internet of Things (DC-IoT)

IGF DC-IoT report 2023

This report summarises the activities of the Dynamic Coalition (DC IoT) since its session at eh Internet Governance Forum in Addis Ababa in December 2022 until the end of 2023.

Background DC IoT

The first meeting of IGF stakeholders that led to setting up the Dynamic Coalition on IoT today, goes back to 2008 and was held in the context of the 3rd IGF in Hyderabad. Since the IGF in Hyderabad, the Dynamic Coalition on the Internet of Things (DC-IoT) has engaged in open meetings at all following IGFs and at meetings in between IGFs. Focus was on the usefulness of Internet of Things, its necessity to help address global and local societal challenges, and the challenges that need to be addressed in order to ensure the Internet of Things is developing in a way that serves people around the globe.

During the IGF meeting in Istanbul (2014) the following issues were put on the table (see 2014 meeting report): the need to ensure privacy, security, ethics, and spectrum issues, and to develop standards that take both social and economic sustainability of networks into account. Networks should be developed in a way people want (people centric values) and in such a way that upgrades, changes of services providers and new applications are possible and affordable.

This led to a discussion that lead to a first version of the IoT Global Good Practice paper published n 2015 and discussed during the IGF in Joao Pessoa, as a vehicle to increase our common insight in how global good practice for IoT looks like. During the successive IGFs the DC IoT continued to further reflect on this paper, and in the Open Meeting during IGF 2018 in Paris DC IoT participants concluded that understanding that legislation alone will not be able to guide development, and may even hamper innovation (if too restrictive, aiming to prevent further damage to society and citizens). This resulted in a call for industry and the technical community to comply with the IoT global good practice principles as reflected in the IoT Global Good Practice paper. It invited all stakeholders to further “spread the word” and have a continued dialogue on good practice, considering the wider application context including Big Data and Artificial Intelligence.

Fast forwarding to the IGF 2022 in Addis Ababa, being the first one where the Dynamic Coalition membership met in person again after the COVID period, we re-engaged in a discussion with a focus on taking stock and looking forward.

Summary outcome of 2023 activities

At the IGF 2023 in Kyoto, the DC-IoT met again in order to progress the work done over the years, linking into the work of other Dynamic Coalitions for as far as relevant to IoT good practice.

Key findings, as reported in the2023 IGF DC IoT Session Report, are:

- IoT data, especially AI-enhanced, should be understandable, accessible, interoperable, reusable, up-to-date and clear regarding provenance, quality and potential bias.
- At the level of devices, there need to be robust mechanisms for finding, labelling, authenticating and trusting devices (and classes of devices). These should survive retraining, replacement or updating but be removable when necessary for functional, security or privacy reasons. To ensure IoT functionality, trustworthiness and resilience, market information and incentives should be aligned. Labels provide a powerful tool; many countries have developed and adopted IoT trust marks, and the time has come to start working towards their international harmonisation.
- Functions are not all confined to single devices, designed in or provided by system integrators; they can also be discovered by end-users or emerge from complex system interactions in cyber-physical systems (CPS) and IoT-enabled services. Governance requires methods for recognising, protecting and controlling these functions and their impacts.

Aim is to build on these findings in 2024 by continued dialogue involving all stakeholders, and making best use of regional IGF opportunities for dialogue.

2023 Activities that lead to this conclusion

Aim was to work towards updating the IoT Global Good Practice Paper that came out of ; organized at the following regional IGFs during 2023:

EuroDIG

At EuroDIG, it was recognized that new development is that IoT enabled networks and services are increasingly autonomous, guided by those data and algorithms that determine what additional data sensors will collect and what actions actuators will carry out. With all that, it is clear that security and stability are becoming increasingly important. Having a clear common understanding of global good practice is key – and in view of all the new developments in technology and society it is crucial we progress that understanding to embrace transparency, accountability, privacy, and security.

The roundtable benefited from introductions on a number of specific topics relating to the evolving practice with IoT, and led to sessions at the annual IGF including:

- The need for a focus on “security by design”, the power of procurement, a taxonomy and also the do-it-together element and the duty of care which is basically for every player in the value chain: what should be expected from which player;
- Recognizing the importance of Core Internet Values, as to avoid that new uses of the internet and the overlay networks will actually hamper interoperability. New developments should be guided by these principles as to ensure continued interoperability – and ensure systems to be robust and resilient against mistakes (“fool proof”);
- Even more so with the emergence of AI than before, it is crucial who in the chain is at least partially liable for the damage and for the risk related to the use of AI enabled IoT, as that enables norms to come in place. People want to know what the potential risk is, what the potential cost factors are. If it is clear who's liable, that creates an incentive for regulation to emerge;
- Usability needs to be already considered at the design phase. For this, it is crucial to involve the local users in the design of the IoT devices to be used in that specific region. For many regions, this means capacity building within the region is key.

Key take-aways:

- with regards to AI the main challenge is in transparency regarding “how it works” and assigning of liability, wherever you come. Clarity on that is needed for people to take their responsibility. Duty of care is key, but if unclarity means one can get away with it, people are less likely to take that responsibility seriously than if they can't get away with it because it's transparent and there's a clear assignment of liability.
- The role of governments is important, and good progress may merit in particular also from governments leading as responsible purchasers of goods and services – i.e. translate that values and needs into government procurement and lead by example – up and beyond the other tasks government have.
- Let's not try to solve the problems of today – as the challenges are dynamic and will continue to evolve over time.. Let's think ahead a little bit about where the future goes when we take that into account.
- Design can make so much difference. Machines get replaced over time and get better. So by ensuring better addressing of our needs “by design”, we gradually changed the version environment where we would be better able to deal with it, too.
- Education came up as essential. With that, an important question raised was: "So where do we go for the right information, establishing of sources of truth platforms where you truly come together?";

African IGF

Internet of Things Good Practice aims at developing loT systems, products, and services taking ethical considerations into account from the outset, in the development, deployment and use phases of the life cycle, thus finding an ethical, sustainable way ahead using loT to help to create a free, secure and rights enabling based environment: a future we want .

These practices include: (1) meaningful transparency to users; (2) Users' ability to understand and exert appropriate control over personally identifiable information; (3) Adequate Security against unauthorized use or access of data on devices; (4) Privacy: adherence to legislation and global privacy practices and: (5) doing so in a way that supports a sustainable way forward with the world.

Specifically in the African context, it is important to ensure an understanding from the continent's perspective on ethical, legal, and social implications of artificial intelligence, Internet of Things (IoT), and other emerging technologies in Africa.

We concluded:

- IoT is important to Africa, in particular in relationship to pursuing the UN's SDG's. Technology is crucial in being able to address SDG objectives, yet when IoT devices and systems are designed for use in the African environment, user needs will need to be taken into account from the outset.
- This requires capacity building in Africa, and involving Africans in designing and developing IoT systems for regional application. This also includes aspects of data governance, as IoT devices collect massive amounts of data that need to be used, and protected, well (during last year's IGF, in particular concerns were expressed about both privacy, and "data colonialism")

APrIGF Brisbane

This session aimed to contribute to evolve our vision on Global Good Practice for IoT towards 2030, taking into account where we are in IoT deployment, policy and regulatory developments around the world, and the role of AI/ML in governing IoT ecosystems, based on Core Internet Values. Key in this to further develop the concept of what it means to have "meaningful transparency" to all stakeholders in the chain, and "real accountability" to those stakeholders that can reasonably expected to bear that responsibility. Specific focus was on (1) introduction of global good practice in IoT; (2) Explanation why approaching it as "Internet of Functions" can help; and (3) focus on the need for labeling (and thus certification) to help consumers to be able to take their responsibility.

The session led to the following take-aways:

IoT is merely an aspect of the internet, just like social networks and communication access to the information. But it does have specific characteristics. It stores, it collects, it stores information, it provides access to many data. Conclusion of the meeting was that we have to embrace IoT to address societal challenges in an ethical way, in a way that encourages investments, and in a way that it is accessible for all that need IoT enabled solutions to deal with societal challenges as well as business opportunities;

When considering the Internet as a network of networks, which must be interoperable through the Internet Protocol (IP), cybersecurity is a first "must" to be able to use it responsibly. Adding the Internet of Things is a step towards an Internet of Functions – functions that also determine the needed level of cybersecurity. When doing so on a global level, it is key to adopt an approach of "zero trust". With regards to zero trust, it will be important to recognize (1) independency of apps from hardware (Internet of Functions); a data centric approach with transparency for Who and How to use the data; (3) and integration of Interoperability at the technical level with legacy systems. Security by design, zero trust, and identification as the order of self/group/public help for cyber security is a mandatory requirement in this.

Certification and labelling are key: however, this cannot be static, binary labels, check marks or star ratings as cyber security is only as good as the day a vulnerability is not discovered or disclosed. Voluntary, industry led or self-regulated labels must not be construed by consumers that the product will have no vulnerabilities for its lifecycle. It is imperative that global programs are set up that are independent, that the method of vendors product conformity assessment is clearly communicated to consumers, and that these bodies of work are scalable and harmonised to be globally applicable

IGF Kyoto

The discussion during the IGF in Kyoto addressed all the above risen issues, and had a well informed debate with global experts on the issues from all stakeholder groups.

Based on the regional IGF discussions, the meeting in Kyoto culminated in the conclusion that rapid progress is made that changes the landscape year on year, and that keeping the discussion going and actively engaging with other DCs provides an opportunity to continuously increase the understanding of how good global practices in IoT governance looks like. Three important takeaways from 2023:

- *IoT data, especially* AI-enhanced, should be understandable, accessible, interoperable, reusable, up-to-date and clear regarding provenance, quality and potential bias.
- At the level of *devices*, there need to be robust mechanisms for finding, labelling, authenticating and trusting devices (and classes of devices). These should survive retraining, replacement or updating but be removable when necessary for functional, security or privacy reasons. To ensure IoT functionality, trustworthiness and

resilience, market information and incentives should be aligned. Labels provide a powerful tool; many countries have developed and adopted IoT trust marks, and the time has come to start working towards their international harmonisation.

- *Functions* are not all confined to single devices, designed in or provided by system integrators; they can also be discovered by end-users or emerge from complex system interactions in cyber-physical systems (CPS) and IoT-enabled services. Governance requires methods for recognising, protecting and controlling these functions and their impacts.

In 2024, DC IoT intends to build upon the take-aways from 2023. All stakeholders are invited to continue to contribute at equal footing, as the world needs IoT, and for IoT to serve humanity well, we will need to ensure commitment to global good practice. In the end, it is always about people.

-=(O)=-