INTERNET STANDARDS, SECURITY AND SAFETY COALITION (IS3C)
MAKING THE INTERNET MORE SECURE AND SAFER

IS3C's contribution to the MAG-DC intersessional meeting

On Wednesday 26 June the second Open Consultation intersessional event was organized by the IGF secretariat and the Dynamic Coalition Cooperation Group (DCCG). In this event the intersessional workstreams, Best Practice Fora, Dynamic Coalitions and Policy Networks presented themselves and their work to the IGF Multistakeholder Advisory Group and all other interested participants in the open consultation.

The participants were asked to reflect on the relevance of their work vis-à-vis the IGF sub themes of 2024. DC IS3C was invited to present on two themes: Harnessing innovation and balancing risks in the digital space; and Enhancing the digital contribution to peace, development, and sustainability. Below you find IS3C's contribution and its request to the MAG to start a process that could lead to recommendations on the conditions under which output of DCs can lead to a formal IGF recognition, thus strengthening the IGF overall.

IS3C

First, a short introduction of DC IS3C, should you not be familiar with it. The Dynamic Coalition Internet Standards, Security and Safety (IS3C) has one main goal: making online activity and interaction more secure and safer by achieving more widespread and rapid deployment of existing, security-related Internet standards and ICT best practices. We have presented reports that: 1) compare and rate national Internet of Things policies at the global level, 2) pointed to the huge gap between the demand made on knowledge in tertiary cybersecurity education curricula by industry and the knowledge and skills taught by educational institutions, in which we worked closely with YouthDiggers of 2022, 3) we showed in how far governments and industry use their economic buying power to procure their ICTs secure by design, 4) presented a tool how they can do so by presenting the most urgent internet standards, 5) we have collaborated in a to be published U.N. report on data governance. You can find our reports here: https://is3coalition.org/docs-category/annual-reports/.

1. Harnessing innovation and balancing risks in the digital space

Why is the topic of internet standards deployment so important? The internet is the basis our world runs on. We work, buy, rest and play there. But what is the internet, what makes it work? Many organisations and governments point to the necessity to protect the public core of the internet, but what is that core? You may think it's the (submarine) cables, the routers, the servers and server locations, and you are right, but without the software behind it, it would just be cables and servers. The Internet protocol, the domain name system, the routing protocol, the email protocol are a few examples of these internet standards. Without them the internet does not function. Without them we cannot connect to anything, send no emails, make online payments, watch Netflix, etc.. We can't even make an "old-fashioned" phone call anymore.

It is important to understand, that these standards have one thing in common, they were all created before the masses came online, without the necessity of security. Although we have to marvel at the robustness of these standards, they need to updated, patched. The technical community has provided these updates in the form of new standards, some already over two decades ago. Numbers however show that patching is quite slow.

It's here that the sub themes of the IGF come into view. We all hear of attacks, loss of data, cyberespionage, ransomware on a daily bases. This is not only a threat to innovation, as it gets stolen, but also to peace and development. Why? Many of these attacks are enabled by flaws in the old, pre 1994 internet standards, risks that can be avoided easily by patching the old with the new. One example. Why have most banks not deployed DNSSEC and really on just DNS? Why do they not put pressure on ISPs to deploy anti-spoofing measures? Both would make the life of phishers on phishing expeditions a lot harder, while their customers become instantly far better protected from harm. It is time that these risks become balanced. It is time for the whole world to move away from relying solely on the multi-billion dollar industry of mitigation, towards **the proactive prevention** of attacks. The risk has to become more balanced by moving away from end user responsibility to a shared responsibly of a) sensible use and b) providing secure by design ICTs, whether they be services, devices, software, websites, applications, etc. This is what IS3C's experts work at, to promote wide-spread deployment of said standards and best practices, balancing risks.

2. Enhancing the digital contribution to peace, development, and sustainability

How can the deployment of internet standards contribute to peace and development?

a. Development

Our research into education and skills in cybersecurity training has revealed that there's not only a skills gap, both in hard and soft skills, but also a gender gap and the fact that not enough youths are interested in a career in cybersecurity. As a result the population is aging, creating an age gap. The outcomes are more or less identical across the globe, despite having different challenges at the outset. Our team led by Janice Richardson, has suggested to form a taskforce, we called a hub, under the IGF. This proved a bridge too far but where else can we bring these very different stakeholders together, on neutral ground and on a fully equal footing? This is food for thought if the IGF wants to make itself more relevant in the coming years. The plan is there, the funding however is not.

b. Peace

As I already mentioned, the public core of internet is abused and attacked every day. This not only endangers development but also peace. Besides attacks from criminals, cyberspace is used for all sort of grey area attacks. Closing attack vectors, i.e. the flaws in the domain name system, in the routing and email protocols, etc., and demanding better developed software, deploying IoT security standards in connecting devices, by securing websites, etc., etc. prevents not only loss of data, but also spying in on meetings, and a lot more. Procuring secure by design ICTs will prevent accidents that may lead to escalations. It is not the silver bullet. What it is, is an inversed shot of hail that the attacks often are. Buying ICTs secure by design is the best option forward and IS3C is actively promoting it.

c. IS3C's 2024 tool

Who need to be convinced to deploy or procure secure by design? The decisiontakers in organisations. They need to be convinced of the necessity to deploy internet standards and to buy ICTs secure by design. Looking at deployment numbers, the current arguments do not seem overly successful. IS3C's next tool will be an alternative set of arguments technicians can use to convince their bossed to actually deploy. This will be presented at the IGF 2024.

A more secure and safer internet is an integral part of the internet we want. So our work ties into the overall IGF theme as well. A more secure and safer internet will sustain peace and development.

d. Support and funding

IS3C had hoped to do more in 2024, turning our recommendations into actions, into training curricula for educators, for procurement officers, for policy makers, etc. To start working with consumer organisations. It proves too hard to find the funding to hire our experts, to pay for the support and coordination. And that while, our common future depends on the development of a more secure and safer internet for all its users, to cyber educate our youth and people willing to change in mid-career to become our digital soldiers, as that is what people working in cybersecurity are. The world has to start realizing this.

To achieve our goals IS3C needs active help in several ways, not just financial. If we receive it, our output will make the IGF a place people come to for guidance, for coordination and for strong policy recommendations all organisations in the world can work with to secure themselves, their environment and countries.

3. DC output recognition request

In the past IS3C has asked the MAG how the output of DCs can receive a formal kind of recognition and IS3C has repeated the question today.

In the past two years we see that the DCs have received more attention and it is clear what ambitious output several of them are striving to produce. In 2024 DCs are put forward as an example of the strength of the IGF and what they can contribute to the outcomes of the IGF. For some DCs it could be a justified question to answer: what is exactly the difference with a Policy Network? (aside from secretarial support and MAG approval).

IS3C already adheres to a strong internal governance structure. This includes a public consultation of our draft outcomes and working with volunteer experts who assist in drafting the reports. You can find it here: https://is3coalition.org/docs-category/governance-document/. IS3C would not object to working with the MAG and thus give up some of its independence. It is even willing to accept guidance where topics are concerned, provided we find the necessary funding to do so.

IS3C suggested to ask DCs who are interested to receive recognition of output to identify themselves and for the MAG to create a process that would be not unlike the work currently overseen in BPFs and PNs.

If the IGF is to be strengthened and this is the message that is strongly conveyed by the IGF community, the strength of having DCs must be utilized more. IS3C kindly asked the MAG to consider to take this next step.

Wout de Natris

IS3C coordinator