Summary discussion:

Evidence and measurement in IG: What sort of data and numbers are we talking about?

This theme is the third of three themes discussed in the build-up to the Geneva Internet Conference. The first theme discussed How to overcome IG policy silos on global and national levels, while the second theme discussed Whom do I contact if I want to raise my Internet governance (IG) concern? Each theme was introduced during a webinar, followed by two weeks of forum discussions. The webinar digest and discussion of the third theme is available here. The following summarises the forum discussion on Evidence and measurement in IG: What sort of data and numbers are we talking about?

The theme tackled the challenge – common in many areas of Internet governance (IG) – of the lack of data and evidence. In cybersecurity, for example, we are still in doubt about the number of threats and the size of the losses incurred. The same applies in other IG fields. Without understanding the scope of the problem, it is difficult to discuss possible solutions. We therefore asked: What can be done to bring more evidence in IG, using what concrete tools and techniques? How should an IG observatory, which would gather and prepare such evidence, function?

During the webinar to introduce the topic, the Internet Governance Forum (IGF) was identified as a possible model for a one-stop shop, or clearing house. In his reaction, **Seun Ojedeji from Nigeria** agreed that the IGF possesses the required attributes, especially since there have been many achievements as a result of the IGF. However, the fact that the achievements and impact are not centrally documented makes it difficult to reference or provide useful case studies. He proposed a coordinated process of sharing success stories that have emerged as a result of IG policy/recommendation implementations at regional level. While noting that all stakeholders have a role to play in this, their individual role is proportionate to their access to resources.

Stephanie Borg Psaila from Malta said that it seemed ironic that in a day and age where the collection of vast amounts of user data appears to be the norm, there is still a lack of data to inform policy-making in many areas. Is it because the data does not exist, or because the data is inaccessible? Where data does not exist, stronger efforts to build awareness and capacity are required, especially among bodies which, given the resources, are placed in a good position (infrastructure, legal) to collect and store the data. Where the data exists, principles of openness, transparency, and accountability need to be instilled. Cybersecurity is possibly one of those areas where these principles alone are not sufficient, as reputation and trust are big risk factors; in these areas, as Dr Gelbstein says in his paper, everyone has a role to play.

Foncham Denis Doh from Cameroon believes that with regard to cybercrime, it is necessary for users to have a platform where they can report cases of cyber threats. Banks need to understand that despite the risk of harming their reputation, the gathering of information about cyber-attacks can actually help prevent more attacks. In addition, with at least one Internet Exchange Point per country, this could be used to monitor traffic and identify cases of fraud at national level. It is important that all actors, from users to content providers, team up to achieve the common goal. Concerning data on online education and jobs, Mr Doh recommends that universities and companies provide compulsory questionnaires to their potential applicants, with simple questions like: Have you ever attended an online training course? Have you ever had an online job? Have you ever had a cyber-attack? These and similar questions can help generate enough data to help us understand what is happening.

In addition to the discussions on the forum, DiploFoundation asked its current IG online course participants to reflect on the theme.

In their reactions, participants agreed that data and evidence, especially on cyber-attacks taking place in their countries, were not immediately available. One participant's comment summarises the common sentiment: 'What I do know is that these attacks happen and it does not appear to me they are properly tracked, documented and responsibly communicated. Organisations like banks are scared of disclosing these attacks considering the huge reputational losses doing this would cause them. Banks in Nigeria, for sure, are taking cybersecurity seriously and are active in investing to be safe and to remain sustainably safe. But cloud storage is challenging them to the marrow as infrastructure sharing, though desirable, is still snagged by pessimism.'