Cybersecurity and the multistakeholder model

Internet governance rests upon a collaborative multistakeholder model, in which governments, private sector organizations, standard-making bodies, NGOs, end-users and academia converse with one another, forge communities and work to ensure that the internet remains a space for innovation and growth. In addition to the significance of this model for the broad dialogue on "classic" topics of internet governance, such as domain name issuance, sustainable growth and access to the internet, internet architecture, freedom of speech and privacy, the multistakeholder model is proving to be extremely relevant for a specific - and unique - area of policy-making and law: domestic cybersecurity.

As countries develop their cybersecurity policy and legislation in order to face growing cyber threats, they are increasingly coming to rely upon multiple levels of dialogue with a diversity of actors in the cyber domain: private sector organizations, ISPs, NGOs, international organizations, and standard-setting bodies. Indeed, given that the cyber domain is intrinsically civilian, governments simply cannot act alone – they need to engage with their stakeholders in a collaborative fashion. For example, in order for CERTs to effectively mitigate cyber threats and respond to incidents, they need to credibly provide – and receive – information from the private sector. At a fundamental level, this requires mutual trust, which must be built from the ground up, through ongoing dialogue and transparent government policies and actions.

This open forum proposes to explore the different ways in which the multistakeholder can and should apply to the world of cybersecurity law and policy. Relevant cybersecurity law and policy experts from Israel and 2-3 other countries could share their experience on how the government-stakeholder engagement has worked (or not) in their jurisdiction, highlighting the advantages and limitations of this model in the formulation and implementation of cybersecurity policy. Representatives of private sector organizations, standard-setting bodies and academia would be invited to share their perspectives as well. The purpose of the open forum would be to allow participants to share thoughts, ideas and best practices on how to make optimal use of the multistakeholder model in the emerging field of cybersecurity law and policy.