Introduction to a Preliminary Report on The Harvard, MIT and U. of Toronto Cyber Norms Workshop 2.0

The workshop Sept. 12-14, 2012, was an opportunity to continue the discussion of some themes raised in last year's workshop and to examine the significance of current cyberspace events and issues for the development of cyber norms and governance.[1] The eight workshop sessions were dedicated respectively to:

- The evolution of the Western model of Internet governance,
- The growing challenges to this model,
- The applicability of international law to cyberspace,
- Particularly the applicability of the Law of Armed Conflict,
- Norms for security and resilience of the telecommunications core infrastructure,
- Issues engaging critical private sector actors in norm development and security awareness,
- Alternative lenses and models for international norms and governance**,**
- Cyber futures and directions for global engagement.

This report consists of summaries for the first seven panels. Because the discussion in the eighth panel involved many voices covering a wide range of points, its summary would have exceeded the length observed by the others. It will therefore be issued as a separate preliminary report.

The workshops have been based on the hope that conversations among cyber policy makers, analysts, academics and practitioners, through their participants' networking and through reports such as this, will inform and support the positive steps by governments, private sector and civil society to promote cyber norms. In order to stimulate the conversations, the workshop format dispenses with presentations of formal papers. Instead, panelists address a series of framing questions for the first forty-five minutes of the session. Discussions are then open to all participants for the next 45 minutes to an hour.[2]

Salient points in the Workshop 2.0 conversations included:

- The multi-stakeholder model of Internet governance and its associated norms are being challenged on both political and economic levels.
- The challenges are part of efforts by many state actors to territorialize their national cyberspace.
- The characterization of the resulting struggle over governance and norms as one of East versus West is too reductionist. There are differences among members on each of these sides. Members of the once called "G77" also have interests of their own regarding governance and norms.
- Despite that struggle, there is near universal agreement on some bases for cyber norms, particularly on the applicability of international law, including the Law of Armed Conflict, to cyberspace. The problem is deciding which laws apply to which to cyber cases.
- The paramount key for a productive, beneficial cyberspace is maintaining trust. Trust can be supported by security architectures, implementation approaches and operational norms.

---

[1] For a report on last year's workshop, see R. Hurwitz, An Augmented Summary of The Harvard, MIT and U. of Toronto Cyber Norms Workshop, May 2012. https://citizenlab.org/cybernorms/

[2] The framing questions for Cyber Norms Workshop are available at https://citizenlab.org/cybernorms2012/

- Motivations, metrics and structures need to be developed collectively across private sector communities and government elements to produce better cyber hygiene, resilience, and action. Such an effort will reinforce the norms and the international civility needed to guide future positive development of cyberspace and its positive evolutionary trends.
- Private sector and civil society organizations have interests and needs in cyber norms that differ from state actors', but they will likely prefer having voices within discussions among state actors, rather than seeking to promote norms on their own.
- The risks to international security stemming from the cyber domain remain high. One scenario under which these risks are reduced is for a "regime" enforced by major cyber players. It could follow from improved cyber defenses, deployed by such actors, which would guard them from threats by less capable actors and leave them at risk only to themselves. They then might reach agreements against the use and proliferation of cyber weapons, similar to those agreements which nuclear capable states have reached on nuclear weapons.
- There is a need to build an epistemic community for cyber security policies. This community would share a common appreciation of the issues and methodologies for analyzing them. Its need is mandated by the complexity of the issues involved and the values put at risk in the absence of a common approach to the cyber domain. Opinions differed, however, regarding the independence from state actors that such a community would need in order to be a credible, effective voice in conversations on cyber norms.

Acknowledgements and thanks to:

Sponsors: The Canada Centre for Global Security Studies, Munk School of Global Affairs, the University of Toronto; The John D. and Catherine T. MacArthur Foundation; Microsoft's Office of Global Security Strategy and Diplomacy (GSSD); The Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government; MIT Computer Science and Artificial Intelligence Laboratory (CSAIL); Explorations in Cyber International Relations (ECIR), a joint Harvard-MIT research project.

My workshop co-chairs Professors Ronald Deibert and Joseph Nye and members of the organizing committee who shaped the agenda and the framing questions for the discussion panels.

The chairs of the panels, named herein, who worked speedily and skillfully with members of their panels to produce summaries that both convey the sense of what was said during the sessions without sacrificing the confidentiality in which it was said.

Notetakers are Camino Kavanagh, Tim Maurer, Sarah McKune and Eneken Tikk-Ringas.

U of Toronto and MIT staff, particularly Irene Poetranto, Maria Rebelo and Ty Seeley

And of course, the participants who made the workshop a stimulating exchange of information, insights and ideas.

Roger Hurwitz, workshop co-chair
Oct. 3, 2012