The Role and Importance of the Multistakeholder Approach

A defining feature of the *Canadian Multistakeholder Process: Enhancing IoT Security* has been its use of the multistakeholder approach in its organization, governance, and decision-making. But what is meant by 'the multistakeholder process'? 'The multistakeholder model' is sometimes referred to as if it were a single solution. But in reality, there is no single model that works everywhere or for every issue. Instead, the multistakeholder approach is an agile set of tools or practices that all share one basis:

> Individuals and organizations from different realms participating alongside each other to share ideas or develop consensus policy.[58]

The Internet Society has characterized the multistakeholder approach as transparent, accountable, sustainable, and—above all—effective. The better the inputs and the more inclusive the process, the better the outputs and the more likely their implementation.[59]

Some characteristics of multistakeholder processes include:

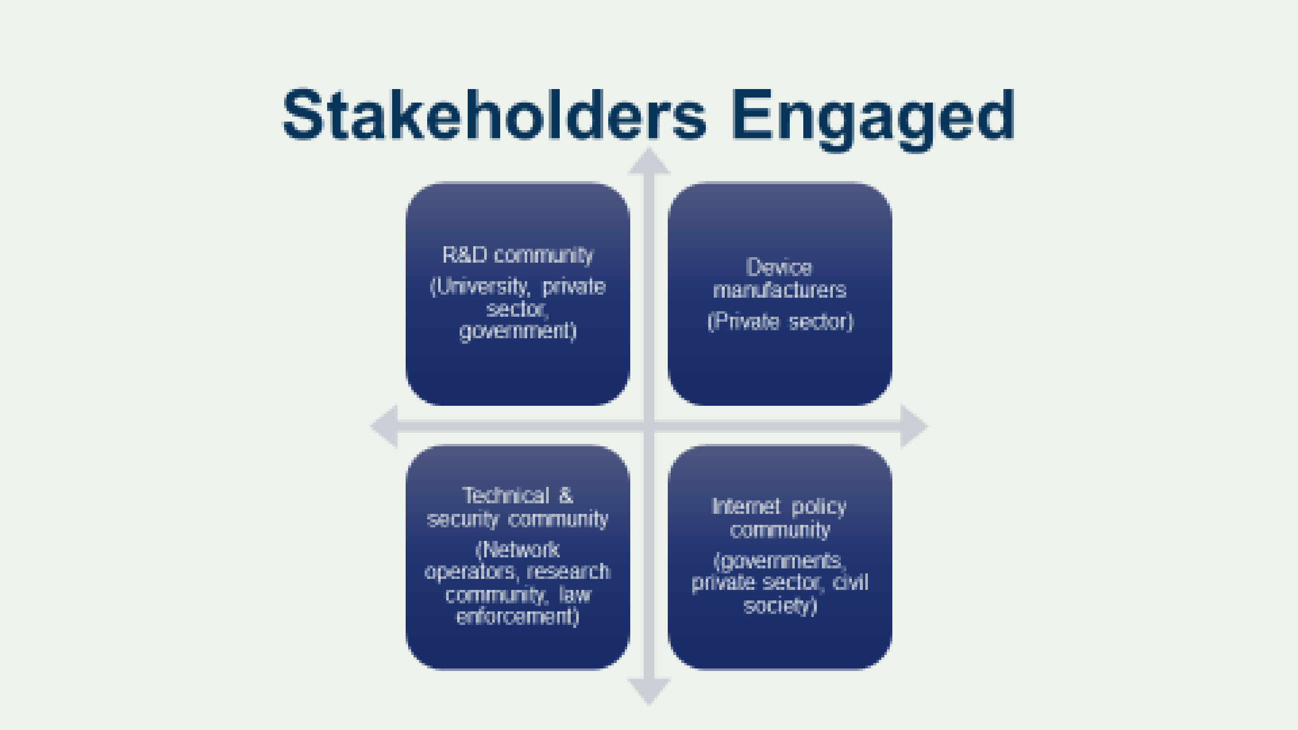
1. All stakeholders have equal permission to speak.
2. Stakeholders self-identify.
3. Stakeholders self-represent.
4. Lack of formal legal procedures.
5. Lack of precedent.
6. Discussion addresses various stakeholders, not just the government.
7. The audience is a participant.
8. State-based entities do not have higher status.
9. Transparency is fundamental.
10. The organization is fluid, but not without structure.

For more than two decades, the Internet Society has been a strong advocate of the use of multistakeholder approaches to policy development and decision-making. Therefore, when it considered the growth and complexity of mitigating cyber security risks from the global proliferation of the Internet of Things (IoT) and the resulting necessity for a "made-in-Canada" policy, it was predisposed to using the multistakeholder model in both the policy development and decision-making process.

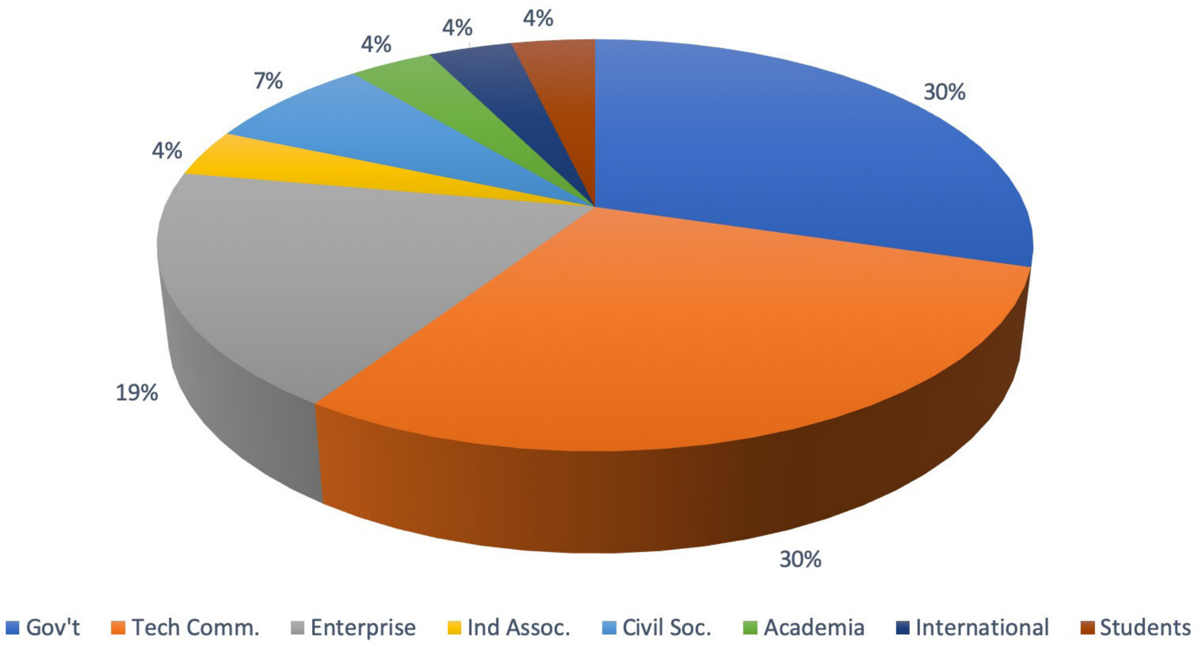
One of the tenets of this model is to engage all stakeholder communities throughout the process, including the technical community, industry, government, consumers, academia, and civil society.

[58] Internet Society, "Internet Governance: Why the Multistakeholder Approach Works". https://www.Internetsociety.org/resources/doc/2016/Internet-governance-why-the-multistakeholder-approach-works/

[59] Ibid.


Stakeholders Engaged
R&D community
(University, private sector, government)
Device manufacturers
(Private sector)
Technical & security community
(Network operators, research community, law enforcement)
Internet policy community
(governments, private sector, civil society)

As the participants in the process engaged in their research, a broader and more diverse group became involved in the process, as indicated below.



This breadth of attendance can be directly linked to the group's openness, its acceptance of new contributors, and its respect of new ideas. Specifically, how did the multistakeholder approach used in this IoT security initiative affect the organization, process, and decision-making?

Organization

The Internet Society convened the process, assuming initial responsibility for setting goals and the agenda, bringing stakeholders together, and ensuring transparency and accessibility. In partnership with the Ministry of Innovation, Science and Economic Development (ISED), they took the initial steps in the process by reaching out to a diverse group of stakeholders from industry, the technical community, government, and civil society. Together, ISED and the Internet Society asked these stakeholders to come together as an Oversight Committee (OC) to structure and support the rest of the process.

The OC included ISED, the Canadian Internet Registration Authority (CIRA), Canadian Internet Policy and Public Interest Clinic (CIPPIC), CANARIE, along with the Internet Society. These primary organizations developed the Enhancing IoT Security initiative and were instrumental in bringing together a much larger multistakeholder group for participation and contribution to the process.

Community Engagement

A transparent multistakeholder group, drawn from the technical community, industry, government, consumers, academia, civil society, and other relevant stakeholders was convened to inform the process, select areas for research, identify appropriate working group members, review documents, and provide guidance to the development of the policy recommendations. Meetings of the Multistakeholder Group were open, public, and livestreamed, with the livestream posted online following each meeting. Reporting to the OC, the convening Internet Society was responsible for managing the process.

Three thematic areas were identified by the larger multistakeholder group and working groups were created for each:

Network Resilience: To develop a set of recommendations to protect the Internet from things and protect things from the Internet.

Device Labeling: To scope out possible labeling regimes that could be applied and/or enhanced in the Canadian landscape.

Consumer Education and Awareness: To establish an education and awareness framework to create a more security-conscious public.

Primary research was conducted through the expertise of members of the Working Groups and insights gained from participating in various fora. All resources from this project were posted on the initiative website in both English and French.

Process

The overall process included moderated, in-person meetings with the larger stakeholder group (half-day and full-day); in between those sessions, there were smaller workshops with special interest groups, virtual roundtables, and bi-weekly webinars. This was supplemented by online communication platforms (Slack, listservs, etc.) for general discussion.

One notable aspect of this process was the contribution from other ongoing and transparent concurrent processes, including the following:

Canadian Internet Governance Forum February 27, 2019

Because many of the IoT security groups were also involved in the organization of the Canadian IGF,[60] one of the panels at this meeting was devoted to "Considerations for Effective Internet of Things Labels." The aim of this panel was to discuss the proposed IoT security framework and how different stakeholder groups can support its implementation, and many of the speakers were participants in the Device Labeling Working Group of the Enhancing IoT Security process. The larger IoT process held one of its face-to-face sessions at the same venue the next day, February 28, and many of the participants in the Canadian IGF participated.

Youth IGF

Youth IGF in Canada,[61] established in 2017, worked with the Internet Society to better engage youth in Internet of Things security and amplify their voices in global and national policy making. As a part of this work, they developed a survey to learn about youth knowledge of IoT security and their opinions are about its future. Results of the survey were used to inform the development of the *Canadian Multistakeholder Process*.

Indigenous Connectivity Summit

The 2018 Indigenous Connectivity Summit[62] (ICS) was held in Inuvik, Northwest Territories on October 11-12, 2018 with the objective of finding solutions to ensure that Indigenous communities across North America can connect to fast, affordable, and reliable Internet. It drew nearly 140 delegates to Canada's Arctic Circle (and included more than 700 virtual participants) for a two-day series of panels and presentations themed on connecting the first 1,000 miles out of communities with a focus on rural and remote northern communities. One of the focus groups at the summit dealt with "Securing the Internet of Things," which was facilitated by Natalie Campbell and Katie Watson Jordan of the Internet Society.

The roundtable discussion resulted in several insights including the view that devices should be built with security at forefront and should be tested and utilize labeling similar to those for organic foods. Security training should be tied into digital literacy training and for many users, security and privacy are viewed as the same. These insights were important both as contributions to the process, and insight into consumers' understanding of the issues at hand.

[60] https://canadianigf.ca/
[61] https://www.facebook.com/YIGFCanada/
[62] https://www.Internetsociety.org/events/indigenous-connectivity-summit/2018/

Norms and Decision-making

At the kick-off meeting of the initiative, Larry Strickling, then Executive Director of the Collaborative Governance Project at the Internet Society and former Assistant Secretary for Communications and Information at the United States' Department of Commerce, began by leading a discussion on the multistakeholder process, including the establishment of ground rules for participation, future discussion, and consensus-building for the group. Participants, both in-person and online, developed the following rules for engagement:

1. Treat people with respect: make sure everyone has a chance to express their ideas, and commit to thinking through and discussing all ideas expressed.
2. Introverts: be proactive. Extroverts: use active listening skills.
3. Stay on topic and be concise and clear.
4. Use "yes, and" instead of "no, but."
5. Raise your hand to speak and do not interrupt.
6. Declare conflicts of interest in advance.
7. Views matter more than numbers.
8. Stick with decisions unless/until new information is brought to the table.

The participants also determined how consensus would be met, with the following criteria:

1. No one is arguing anymore.
2. All dissenting views have been discussed.
3. The majority agrees on a decision, a few can live with it, and none or almost none of the participants cannot live with it.

International Linkages and Outputs

Another important aspect of the Canadian IoT process was the ability of some of the participants to bring the experience of the process to the international community. Examples include:

1. Maarten Botterman, of GNKS Consult BV, in the Netherlands, is also an active participant in the IGF Dynamic Coalition on IoT Security[63] and provided an update on the process at the IGF in Paris in November 2018.
2. Byron Holland, of CIRA, and Taylor Bentley, from ISED, also provided their perspective on the Canadian process at a different panel at the 2018 IGF: Global Alignment for Improving the Security of the Security of IoT Devices.[64]
3. ISED has agreed to participate on the IoT Security Policy Platform to share best practices and harmonize the IoT security landscape along with representatives from the United States, United Kingdom, Netherlands, France, Senegal, Uruguay, Mozilla, ENISA, and others.

International Processes Inspired by the Canadian IoT Process

Senegal – A delegation from Senegal came to Canada[65] in July to meet with members of the *Enhancing IoT Security* oversight committee. The group was comprised of government officials, Internet Society Senegal Chapter members, and staff from the Internet Society's African Bureau. The delegation met with Canadian government officials, technologists, public interest groups, and North American Bureau staff to learn more about how and why the IoT security project was initiated, and what the group had accomplished to date. The group discussed the significant successes the Canadian multistakeholder group had already achieved, the challenges it faced, and goals for the project. These conversations ultimately aided the delegation in its decision to replicate the Canadian process to enhance IoT security in Senegal. On November 28-29, the inaugural Senegalese *Multistakeholder Process: Enhancing IoT Security*[66] was held and a representative from the Canadian initiative presented on the best practices and lessons learned to date in Canada.

France – In January 2019, the Internet Society announced the creation of the IoT Security Working Group.[67] Its founding members include AFNIC (French Association for Internet Naming and Cooperation), ANSSI (National Agency for the Security of Information Systems), ARCEP (Regulatory Authority for Electronic Communications and Posts), CINOV-IT (Professional Chamber of Small and Medium-sized Digital Enterprises), Conseil National du Numérique (National Digital Council), La Quadrature du Net (Squaring of the Net advocacy group), Nokia, and Pôle Systematic Paris-Région (Ile-de-France business cluster).

The Working Group leads are now actively consulting members of the Canadian OC as they develop their best practices and recommendations.

[63] https://www.iot-dynamic-coalition.org/dc-iot-meetings-at-igf/13th-igf-paris/
[64] https://www.intgovforum.org/multilingual/content/igf-2018-of-25-global-alignment-for-improving-the-security-of-iot-devices
[65] https://www.Internetsociety.org/blog/2018/07/collaborative-governance-leaders-canada-and-senegal-exchange-notes-on-iot-security-frameworks/
[66] https://www.iotsecurity.sn/2018/12/senegal-kicks-off-enhancing-iot-security-project/
[67] https://www.Internetsociety.org/news/press-releases/2019/Internet-society-advances-iot-security-in-france/

Lessons Learned

For all of the multistakeholder process' advantages, it also poses challenges. Over the course of this project, the group developed best practices based on what it learned that it will incorporate into future initiatives.

These lessons included:

1. **Scope:** Defined by participants, and if gaps appear, they can only be addressed by the group as a whole in agreement.
2. **Time:** Because multistakeholder projects can move very slowly, adding extra contingency time is prudent.
3. **Stakeholder identification:** Use as many resources as possible to assist with identification and outreach, including the Oversight Committee, newly recruited stakeholders, and the influence of champions within your own organization.
4. **Stakeholder engagement:** Multistakeholder projects demand much commitment from stakeholders.
5. **Facilitation:** The most critical component to this initiative's success has been using a facilitator who is both a subject-matter expert and has experience with the multistakeholder process. In the case of the *Enhancing IoT Security* initiative, that was Andrew Sullivan, President and CEO of the Internet Society.
6. **Maintaining momentum:** After pivoting to more webinars and many more communication platforms, engagement increased between multistakeholder meetings.