SUBMISSION BY INTERNET SOCIETY CANADA CHAPTER IN THE PUBLIC SAFETY CANADA

CANADA'S WAY FORWARD ON CYBER SECURITY CONSULTATION

15 OCTOBER 2016

Table of Contents

1.0 Introduction

1. Internet Society, Canada Chapter[1] ("ISCC") is hereby making its submission in the Public Safety Canada consultation on Canada's way forward on cyber security. ISCC is a volunteer association that seeks to advance the cause of the Internet in Canada. ISCC is a chapter of the international Internet Society[2] ("ISOC"), which is a non-governmental organization that "engages in a wide spectrum of Internet issues, including policy, governance, technology, and development."[3] ISCC has prior and ongoing participation in other government initiated consultations including the recent Global Affairs Canada's Canadian International Assistance Review Consultations and Public Safety Canada's current Consultation on National Security.

2. Some of ISOC's work, in which ISCC participates and that it supports, includes:

- "Championing public policies that enable open access;
- Facilitating the open development of standards, protocols, administration, and the technical infrastructure of the Internet;
- Organizing events and opportunities that bring people together to share insights and opinions."[4]

A complete list of ISOC's mission can be found at http://www.internetsociety.org/who-we-are/mission.

3. ISCC applauds Public Safety Canada for undertaking a consultation on the way forward on cyber security. ISCC has reviewed Public Safety Canada's report entitled "Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security"[5] (the "Discussion Paper") and is encouraged by the key trends, issues and questions identified in the report.

4. ISCC's positions in this consultation are derived from a conference it held in Ottawa on September 19, 2016 to discuss cyber security issues and devise a set of recommendations for Public

---

1 Internet Society, Canada Chapter, "ISOC Canada", <http://www.internetsociety.ca/>.
2 Internet Society, "Internet Society", <http://www.internetsociety.org/>.
3 Internet Society, "What We Do", <http://www.internetsociety.org/what-we-do>.
4 *Ibid.*
5 Public Safety Canada, "Security and Prosperity in the Digital Age: Consulting on Canada's Approach to Cyber Security", 2016.

Safety Canada's consideration. Individuals from a variety of backgrounds attended the conference both in-person and remotely from across Canada.

5. This submission approaches the topic of cyber security primarily from the perspective of the individual Internet users, who increasingly have as much to lose as they have to gain from participation in a digital world. However, Internet users are but one of the many stakeholders on the issue of cyber security, each with their own distinct set of interests. Balancing these interests as optimally as possible is critical to the success of our government's approach to cyber security. To this end, ISCC is recommending that Public Safety Canada establish an active and continuous multistakeholder approach to proactively respond to current and emerging cyber security issues.

6. While the adoption of a multistakeholder approach is the core strategic recommendation of this submission, ISCC is also proposing a list of three specific measures that warrant Public Safety Canada's careful consideration. These options consist of concept policies, initiatives, campaigns, research and other measures. In the ISCC's view, the adoption of some or all of these measures, at Public Safety Canada's discretion, would contribute meaningfully to improved levels of cyber security.

2.0 The Multistakeholder Approach

7. ISOC prepared a report entitled "Internet Governance: Why the Multistakeholder Approach Works"[6]. This concise and practical report: i) explains the multistakeholder approach as it relates to Internet governance; ii) distills the multistakeholder approach to its fundamental principles; and iii) provides illustrative examples of successful implementation of the multistakeholder approach to address current issues. Given the breadth of relevant information in this report, the ISCC has included it as an Appendix to this submission.

8. At the outset, it is appropriate to define what is meant by the 'multistakeholder approach'. As explained in the ISOC report, the multistakeholder model is a set of tools or practices that that all share one basis, namely "[i]ndividuals and organizations from different realms participating alongside each other to share ideas or develop consensus policy."[7] The model is not a static

[6] Internet Society, "Internet Governance: Why the Multistakeholder Approach Works", 2016.
[7] *Id.* at p.5.

solution but rather, an adaptive and flexible approach which channels collective input from interested parties.

9. Of course, the multistakeholder approach is best suited for certain issues with a defined set of characteristics. These characteristics are set out in the ISOC report. Specifically, ISOC concludes that the multistakeholder approach is particularly effective for issues where[8]:

- Decisions impact a wide and distributed range of people and interests;
- There are overlapping rights and responsibilities across sectors and borders;
- Different forms of expertise are needed, such as technical expertise; and
- Legitimacy and acceptance of decisions directly impact implementation.

10. All of the above-listed criteria apply to the cyber security issues that are the focus of this consultation.

11. To demonstrate, consider first that, as aforementioned, decisions regarding cyber security affect a broad range of players[9], including but not limited to: businesses which need to safeguard customer information and protect corporate data and networks; individuals who need to have their personal information protected and who require a sense of security to reap the full benefits of the digital economy; and governments who must protect national security and the security and privacy of its citizens.

12. Second, the rights and responsibilities of these cyber security stakeholders are intensely intertwined. Each player has a vested interest in shaping cyber security policy. Likewise, each player shares a responsibility for protecting and enhancing cyber security going forward.

13. Third, a very diverse set of expertise is required to address cyber security threats. For example, a comprehensive approach to cyber security threats would require extensive technical, legal (judicial and law enforcement), policy and advocacy expertise.

14. Fourth and finally, the acceptance and perceived legitimacy of decisions affecting cyber security is directly correlated by the process leading to the implementation of such decisions. In

---

8 *Id.* at p.2.

9 These stakeholders were referenced in an ISOC article entitled "Internet Society Approach to Cyber Security Policy" dated 22 January 2015 available at <https://www.internetsociety.org/news/internet-society-approach-cyber-security-policy>.

other words, stakeholders will be far more likely to accept, implement – and ideally, embrace – cyber security decisions if they have an opportunity to contribute to the decision-making process.

15. Having defined the multistakeholder approach and determined that this model is indeed best suited to address cyber security issues going forward, the focus now turns to how the model should be designed and implemented for cyber security.

16. Conveniently, this consultation is a perfect launching point to set the foundation for a multistakeholder strategy. Public Safety Canada will have a fulsome record, based on its consultation, that will serve to identify stakeholders, issues (including priority threats and risks) and potential measures that could serve to bolster cyber security in Canada going forward. Understanding the issues and the stakeholders that are affected by them must necessarily be the first priority. An in-depth understanding of the problem is critical to designing an effective strategic response. Once this knowledge base is established, the next step is to determine a set of characteristics that a multistakeholder approach must have to successfully deal with cyber security issues.

17. A key characteristic of the approach must be adaptability. The Internet and technology more broadly are constantly evolving in profoundly innovative and unpredictable ways. Cyber security threats evolve in step with, and perhaps even ahead of, this rapid and constant march of technological progress. For this reason, an effective multistakeholder approach must be flexible and adaptable to unforeseen changes in the cyber security landscape. The strategy going forward must also be active and continuous. This is a consequence of the ever-evolving nature of cyber security threats. A solution that produces regular input from stakeholders can result in timely preventative (e.g. warnings to consumers or distribution of a software vulnerability patch) or restorative (e.g. services for consumers affected by a privacy breach) measures. In contrast, if the outcome of this consultation is a set of stand-alone policies rather than an ongoing multistakeholder strategy, protections against cyber security threats could quickly become obsolete and fixes thereafter might be difficult to organize and implement.

18. In addition to being adaptive, active and continuous, the multistakeholder model should also be inclusive, open and transparent.[10] As explained by ISOC, inclusiveness is the basis of

[10] *Supra* note 6, at p.5.

legitimacy in collaborative decision-making.[11] The less inclusive a process is, the less likely it is to engender the trust and support of those outside of the process.[12] As a starting point, an initial list of stakeholders can reflect the participants in this consultation as well as certain other key parties whose mandate or interests are closely linked to cyber security. Invitations to participate can be sent where necessary. Otherwise, applications to join the process should be reviewed on a timely basis with a view to inclusiveness. When it comes to transparency, the multistakeholder model should ensure transparency of inputs, process and decision-making.[13] The model should strive to achieve a decision-making process that is clear, robust and accessible from beginning to end, for sophisticated and non-sophisticated participants alike. This commitment to open and transparent practices should, in turn, encourage the development of a shared sense of collective responsibility among the stakeholders.[14]

19. Without full insight into the final record of this consultation, it is difficult to propose exactly how a multistakeholder model with all of the above features and qualities could be implemented in practice. Ultimately, only Public Safety Canada will be in a position to make such determinations. However, ISCC wishes to submit certain ideas that may be of assistance.

20. The decision-making process could be organized through the creation of a number of committees and sub-committees, each with a defined role and set of responsibilities. There are a number of possible ways to organize such committees. One way would be to assign a committees based on key cyber security topics. For example, this approach could lead to the establishment of: A Privacy Committee to deal exclusively with cyber security issues affecting the privacy and access to personal information of Canadians; A National Security and Cross-Borders Committee to manage matters related to foreign cyber security affairs and national security; and an E-Commerce Committee to deal with business, corporate and commercial cyber security issues, etc. The advantage of this structure would be that each committee would be generally focused on a narrow set of topics. As a result, discussions might tend to be more streamlined and decision-oriented. Another effect of this structure might be that committees will attract disproportionate participation from stakeholders with vested interests. While this could translate in the availability

[11] *Ibid.*
[12] *Ibid.*
[13] *Ibid.*
[14] *Ibid.*

and development of valuable expertise for each committee, it might also detract from the multistakeholder strategy. Safeguards might therefore be warranted to ensure that each committee benefits from equal representation of a diverse set of stakeholders.

21. An alternative and perhaps superior approach would be to organize committees based on well-established corporate governance models. For example, a Policy Committee could be tasked with developing policies on all cyber security issues based on stakeholder consensus. An Implementation Committee could coordinate the development and implementation of programs and measures to address cyber security issues, once such measures are approved by consensus of the Policy Committee. A Membership and Outreach Committee could be tasked with engaging stakeholders and encouraging participation. Various other committees could be created, as necessary, to fulfill each step of the decision-making process and ensure the organization and efficiency of the multistakeholder approach going forward. Overall, this structure promotes inclusiveness and openness more naturally. Many stakeholders would have familiarity with this form of governance due to its general similarity to commonplace organizational governance models. The model would also be accessible and easy to understand for stakeholders who do not happen to benefit from such familiarity. Most importantly, this structure is more likely to consistently draw perspectives from all participants, on all issues. For this reason, ISCC submits that a committee subdivision based on governance functions is most compatible with the multistakeholder approach.

22. Terms of reference can be created to draw appropriate boundaries to the powers and responsibilities of each committee. Such terms of reference must also ensure that committees are not granted any power which properly rests within the exclusive jurisdiction of a branch of government. However, each branch of government is free to participate in committee work and is indeed encouraged to do so. In fact, the participation of certain government actors will be critical to the success of a multistakeholder approach to cyber security. Some of these government actors are named below, in a concept list of stakeholders and stakeholder groups.

23. In the ISCC's view, stakeholder participation should include federal representatives from Public Safety Canada, Innovation, Science and Economic Development Canada, the Office of the Privacy Commissioner, federal law enforcement agencies and several other government departments and agencies. Provincial governments should also participate actively, especially with

respect to matters that are related to education (e.g. development of public awareness through school programs) and provincial privacy legislation, if applicable. Extensive non-government participation would be expected from technology firms, businesses, financial institutions, telecommunications service providers, consumer and special interests groups and academia.

24. Committees could meet regularly as often as necessary (e.g. weekly, bi-weekly, monthly or bi-monthly) and ad hoc meetings can also be arranged to deal with urgent issues. On a semi-annual or annual basis, a general meeting of stakeholders can be held to reassess and improve the decision-making process and committee structure, as necessary.

25. For the reasons outlined throughout this section, ISCC urges Public Safety Canada to adopt a multistakeholder approach to cyber security issues going forward. The preceding paragraphs propose a few ideas that could be applied to organize such a model. However, it may also be appropriate to launch a follow-up consultation, on an expedited basis, to invite additional submissions with regards to the most appropriate and effective multistakeholder structure going forward. This will undoubtedly elicit valuable ideas and examples that could meaningfully assist the design and implementation of the multistakeholder model.

3.0 Specific Recommendations for Addressing Cyber Security Issues

26. As noted at the outset of this submission, ISCC's September 19th cyber security event garnered substantial feedback from online and live participants on cyber security issues. Participants discussed the most pressing cyber security issues from their perspective as well as potential solutions to those issues. ISCC has distilled this feedback into a list of three sets of recommendations for addressing specific cyber security issues. Pending any further consultation (whether or not involving a multistakeholder approach), the sections that follow address ISCC calls for greater education, public awareness and support resources for victims of cybercrime. The recommendations are not presented in any particular order and could be adopted individually or as a whole.

3.1 Government Department for Victims of Cybercrime

27. Participants at ISCC's cyber security event agreed there is a significant lack of information and support resources for individuals who have been victimized by cybercrime. Persons who have been subject to identity theft or fraud over the Internet often do not know what steps to take or who to contact. The process to remedy the damage caused by cybercrime and prevent further loss is complex and overwhelming for most people. Although guidelines[15] detailing what to do if a person suspects that they have been a victim of identity theft or fraud are available on the Internet, there are few comprehensive resources that a person can access for assistance and support that is tailored to their specific circumstances. The fraud guidelines and information that are available tend to be decentralized or fragmented (e.g., credit card fraud guidelines are posted on the related financial institution's website[16], drivers license[17] and health card[18] fraud guidelines are posted on separate government websites, etc.) and overloaded with phone numbers, fillable reporting forms, URL links and other information and contact coordinates.

28. Quick and decisive action is critical to mitigating additional harm once cyber fraud has occurred. Canadians require a centralized and comprehensive cyber fraud support resource. Accordingly, ISCC recommends the establishment of a government department dedicated to this purpose. This 'Department' could be federally run, perhaps as a restructured and revitalized Canadian Anti-Fraud Centre. The Department would be responsible for providing real time assistance to victims of cybercrime. After assessing each individual case in detail, this assistance could take the form of a case-specific, concise and accessible list of simple steps and single points of contact to prevent further harm and remedy harm that has occurred. Ideally, each of these steps should be facilitated by the Department to the greatest extent possible. Wherever coordination is required with provincial government departments or law enforcement agencies, the Department could create and forward an incident report to these entities for reference, thereby expediting the

---

[15] See for example the information on the Canadian Anti-Fraud Centre website: <http://www.antifraudcentre-centreantifraude.ca/fraud-escroquerie/index-eng.htm>; See also, for example, the Employment and Social Development Canada website detailing steps to take if a persons suspects that someone is using their SIN: <http://www.esdc.gc.ca/en/sin/protect.page>.

[16] See for example: https://www.tdcanadatrust.com/products-services/small-business/merchant-solutions/fraud-awareness/fraud-awareness.jsp.

[17] See http://allontario.ca/2013/05/preventing-driver-licence-fraud/.

[18] See http://www.health.gov.on.ca/en/public/publications/ohip/card_fraud.aspx.

cybercrime victim's subsequent interactions. The Department should also actively follow-up with the victim multiple times in the immediate days following the crime in order to monitor progress and assist with any difficulties.

29. In ISCC's view, this proposal would provide victims of cybercrime with an invaluable resource to work themselves out of a situation of vulnerability. This end-result surely warrants the allocation or re-allocation of federal funding.

3.2 Academic Research and Statistics

30. The government should consider commissioning a special constitutional / human rights study of policies governing online behaviors including cybercrime. A constitutional scholar could apply a multidisciplinary approach to assessing various constitutional questions and topics that ought to be revisited in light of the advent of technology and the cyber security issues that come with it. This research could assess: the meaning and scope of constitutional powers in a digital world, correct models of constitutional institutions and the correct approach to constitutional powers and rights. One notable point of focus could be the meaning and implications of the *Canadian Charter of Rights and Freedoms*[19] and in particular, the Section 7 Charter rights of life, liberty and security of person vis-à-vis cyber security topics such as privacy.

31. ISCC submits that the constitutional research contemplated above would provide valuable academic insight into complex issues that are not currently fully understood. Furthermore, this research can assist Public Safety Canada in identifying policy gaps and adjusting its cyber security strategy accordingly.

32. For similar reasons, the government should commission statistics research to further its understanding of the magnitude and prevalence of cyber security threats. Statistics gathered by a national survey could track the number, type, frequency of cyber security incidents. Also of interest would be information relating to the victims of cybercrime, such as age, education and geographic location.

[19] The Constitution Act, 1982, Schedule B to the Canada Act 1982, 1982, c 11.

3.3 Public Awareness Campaign

33. Participants at ISCC's cyber security event proposed the launching of a cyber security public awareness campaign. Drawing inspiration from successful national and international public health campaigns (e.g. anti-smoking and hygiene / "clean hands" campaigns), participants submitted that an edgy, captivating campaign could encourage Canadians to take proactive measures to protect themselves from cybercrime.

34. A cyber security awareness campaign could revolve around a poignant slogan or catch-phrase and involve:

- Television, radio, website, newspaper and public billboard advertisement and messaging emphasizing the risks and harms of unsafe web activities;
- Disseminating simple and effective tips for staying safe online (e.g. a "top 10" list of measures that everybody should take when online) through the channels listed in the above bullet point;
- Labels on computer and networking hardware and software (when sold physically and by way of click-through notices if downloaded online) reminding users of the risks and precautions that should be taken when utilizing such products online, perhaps with a link to further information;
- Changes to education curriculums to teach safe online practices to young users of the Internet; and
- Public information sessions at libraries, universities and schools to teach safe online practices and direct attendants to additional resources.

35. In ISCC's view, a widespread campaign that is spearheaded by government and promoted by cyber security stakeholders could translate into substantial adoption of preventative measures. Effective public awareness initiatives will not only inform Canadians about both the risks associated with online activities and measures that can prevent such risks from materializing – but also convince Canadians that changing their habits can pay off.

4.0 Conclusion

36. In the Discussion Paper, Public Safety Canada identifies the following five principles for a renewed cyber security approach[20]:

- Protect the safety and security of Canadians online and of Canada's critical infrastructure;
- Promote and protect rights and freedoms online;
- Recognize and encourage the importance of cyber security for business, economic growth, and prosperity;
- Collaborate and coordinate across jurisdictions and sectors to collectively increase Canada's cyber security; and
- Adapt to respond to emerging technologies and changing conditions.

37. ISCC agrees wholeheartedly with these principles. Fulfilling each of these principles will require a collaborative approach that is capable of balancing diverse and sometimes competing interests. To ISCC's knowledge the only proven model to achieve such a goal is the multistakeholder approach.[21]

38. Complementing a multistakeholder approach with the recommendations regarding greater education, public awareness and support resources for victims of cybercrime outlined in Section 3.0 of this submission would contribute greatly to attaining security and prosperity in the digital age.

39. ISCC thanks Public Safety Canada for the opportunity to participate in this consultation and remains committed to fulfilling its role in promoting cyber security in Canada.

[20] *Supra* note 5, at p.22.
[21] *Supra* note 6 at p.2-4.

APPENDIX

Internet Governance

Why the Multistakeholder Approach Works

Executive Summary

- The multistakeholder governance framework is informed three components: a) opened-ended unleashed innovation (*infrastructure*), b) decentralized governance institutions (*governance*) and, c) open and inclusive processes (*human*).
- The Internet is open, distributed, interconnected, and transnational. The multistakeholder approach to Internet governance has grown from the Internet's own DNA and is what allows it to thrive.
- Multistakeholder approaches are used in many areas as an accepted international norm. In the Internet area, as in other areas, the multistakeholder approach is widely accepted as the optimal way to make policy decisions for a globally distributed network. This is reflected in declarations, resolutions, and day-to-day working practices of a growing number of international organisations.
- Multistakeholder decision-making is accountable, sustainable and – above all – effective. The better the inputs and the more inclusive the process, the better the outputs and their implementation.
- Just as the Internet is evolving, and the digital economies and societies that rely on it, the multistakeholder approach must adapt to meet new challenges.
- The Internet Society has developed four attributes of successful multistakeholder decision-making to guide the next phase of its evolution: **inclusiveness and transparency; collective responsibility; effective decision-making and implementation; collaboration through distributed and interoperable governance.**

We get better answers to global questions when a range of experts and interests can meaningfully take part in the discussion.

The multistakeholder approach is a toolbox, not a single solution

Many people talk about 'the multistakeholder model' as if it is a single solution. But in reality there is no single model that works everywhere or for every issue. Instead, the multistakeholder approach is a 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.

Compare two building materials: concrete and bamboo. Concrete is rigid and inflexible. We need it to build tall, but on its own it cannot survive great shocks. Bamboo is surprisingly strong and, crucially, flexible. Used in the right place, bamboo can carry weights many times its own. The multistakeholder approach is a little like bamboo. It is nimble, adaptable, and stronger than it may first appear.

Why use the multistakeholder approach?

The multistakeholder approach has been used for everything from allocating fair fishing rights to digitising land registries to developing a code of ethics for an international organization. It works best on issues where:

- Decisions impact a wide and distributed range of people and interests,
- There are overlapping rights and responsibilities across sectors and borders,
- Different forms of expertise are needed, such as technical expertise, and
- Legitimacy and acceptance of decisions directly impact implementation.

The multistakeholder approach allows us to protect and further develop the complex systems we rely on while allowing those systems to go on working.

The Internet and the multistakeholder approach

The Internet was developed by the public and private sectors, academia, and civil society, harnessing the shared technical expertise of a global community of equals. Today, much of the Internet's infrastructure is operated across borders and by a range of different stakeholders. It is a complex but robust ecosystem where each part of the Internet can rely on many other parts working together but often independently.

Key Internet principles have made the Internet a global platform for innovation and economic growth:

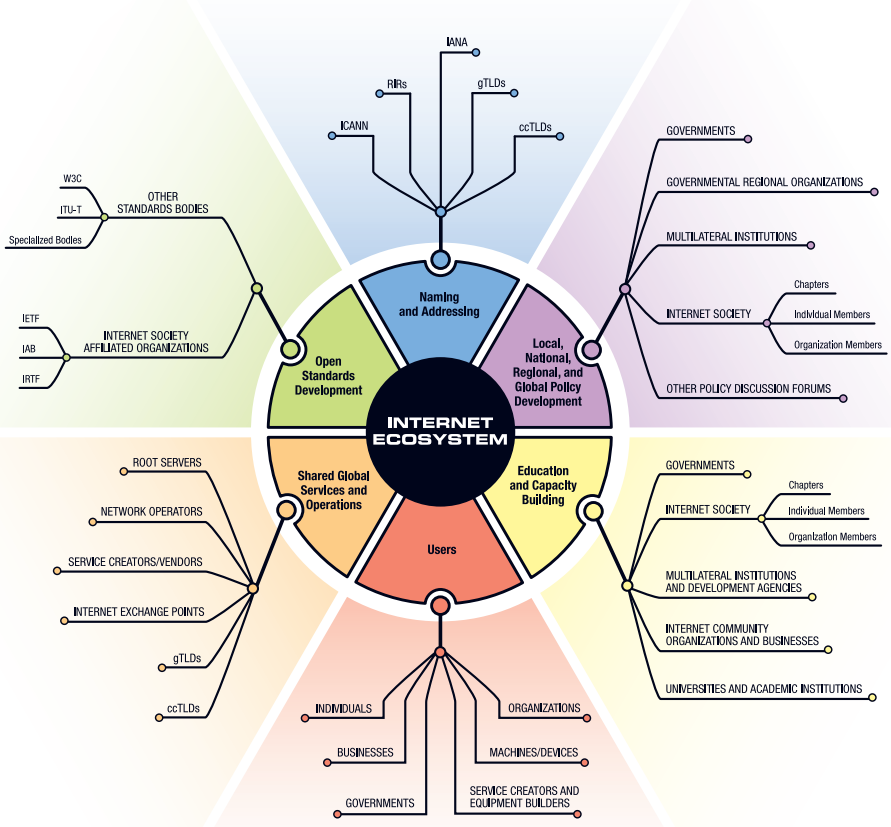
- Participatory bottom-up processes,
- Prioritising the stability and integrity of systems, and
- Maintaining the open nature of the underlying technologies.

Those principles are not 'add-ons' but are part of the Internet's DNA.

The Internet governance ecosystem

The Internet's governance reflects the Internet itself: open, distributed, interconnected and trans-national. Just as the Internet is interoperable, so are its governing parts.

Fig. 1 The Internet's governance arrangements are an ecosystem



MS IN ACTION

IANA Transition

The Internet Assigned Numbers Authority (IANA) administers some unique Internet identifiers, including Internet Protocol (IP) numbers. It also keeps a public record of the 'root zone', the record of operators of top-level domains such as .uk and .com. It is run by the Internet Corporation for Assigned Names and Numbers, ICANN, under contract to the U.S. government.

In 2013, the leaders of many technical Internet organisations, including the Internet Society, called for the globalization of the IANA functions, and for all stakeholders, including governments, to be able to participate fully in the process to formulate a proposal for the transition of the IANA functions away from the US government's oversight.

In 2014, the U.S. government asked the global Internet community to make a plan for moving IANA's oversight to the global, multistakeholder community.

Public and private sector organizations, technical experts, and civil society representatives from around the world organized themselves groups to work on the plan.

For more than two years, people worked collaboratively at over 600 meetings and conference calls, sending over 32,000 mailing list messages to create a new, fully global and multistakeholder transition plan.

In March 2016, the proposal was endorsed by all stakeholders, including ICANN's Governmental Advisory Committee, and is now being considered by the U.S. government. The plan shows how the multistakeholder approach worked to create a stable, secure, accountable, and transparent way to manage a critical Internet resource. Just as the Internet is a 'network of networks', so its global governance is a set of overlapping organisations with different roles and ways of working.

The way these organizations make consensus decisions still reflects the Internet technical community's defining principles – openness, end-to-end networking, and, above all, effectiveness.

Increasingly, the public and private sector organisations that rely on the Internet are adopting not just Internet technologies, but the 'Internet way of doing things': the multistakeholder approach.

International organizations are adopting multistakeholder approach

Multistakeholder decision-making started as a form of collective decision-making that allowed the Internet to evolve. It is a driving day-to-day work and strategic direction in what we used to think of as largely intergovernmental decision making bodies.

In 2005, the United Nations General Assembly agreed to organise the World Summit on the Information Society (WSIS) in a multistakeholder way. Since then, many international and multilateral organizations have publicly endorsed the multistakeholder approach as the way to do Internet governance:

- 2008 – Organisation for Economic Cooperation and Development (OECD)
- 2009 – The Council of Europe
- 2010 – International Telecommunication Union (ITU) Plenipot
- 2011 – G8 at Deauville
- 2014 – NETmundial meeting in Brazil
- 2015 – UN General Assembly WSIS+10 High Level Event: re-endorsed the multistakeholder approach and the Internet Governance Forum (IGF).

The multistakeholder principles that have made the Internet such a success are increasingly being used in the Internet's policy and governance work. They are now an accepted international norm for how the Internet is governed.

But the multistakeholder approach itself is evolving and needs to continue evolving. Academic research has identified many ways in which multistakeholder decision-making can and should evolve. It is time we put that into practice.

The harder and more interconnected the problem, the *more* multistakeholder the path to the solution needs to be.

MS IN ACTION

OECD Security Guidelines

In 2013–2015, the Organisation for Economic Co-operation and Development (OECD) revised its security guidelines. Although largely member country-driven, the OECD has defined roles for business, civil society, trade unions, and the Internet technical community. Recognising that digital security risks cross sectors and borders, the new guidelines promote an even stronger multistakeholder approach.

Stakeholders agreed that digital security is an economic and social issue, not just a technical issue, and that all stakeholders are responsible for managing digital security risk, according to their role and the context. Further, they encourage cooperation across sectors, stakeholders, and borders.

In 2015, the OECD Recommendation *'Digital Security Risk Management for Economic and Social Prosperity'* was widely praised for its extensive relevance across.

What were the keys to success?

Clear, shared goals – The OECD ran multistakeholder expert consultations with OECD and non-OECD countries, the four recognised stakeholder communities (BIAC, TUAC, CSISAC, ITAC) and invited experts to understand the security landscape, define objectives and outline core principles. Focused goals helped build consensus and kept the review on track.

Culture of mutual respect – Stakeholders explicitly shared a commitment to finding solutions that work, giving digestible and factual input, and respecting each other's perspectives and time. The Secretariat's active drafting (as an neutral participant) and coordination were also crucial.

Self-organised stakeholder groups generating collective input

Building on existing structures and relationships – The OECD's *Internet Policy Principles* already showed that multistakeholder approaches work best on Internet issues. The OECD built on its existing stakeholder relationships to tackle cross-border and cross-sector security together. Multistakeholder approaches meshed well with existing structures to improve the quality of the result and help its wide adoption in OECD countries and beyond.

A framework for ongoing improvement of decision-making

What is it about the multistakeholder approach that makes it so useful, robust, and adaptable? And how can we make sure it continues to successfully answer the most complex questions of our globally interconnected and interdependent world?

Just as the Internet needs to reach the next billion people, the multistakeholder approach needs to continue evolving so that it can solve the problems of the next decade and the next century.

The Internet Society has come up with a list of attributes for multistakeholder decision-making. Our focus is on how it can best be done, not in idealising a perfect model. This is because we believe multistakeholder decision-making is a set of behaviours and practices that can be applied almost anywhere. They will make each organisation or process's ways of working more robust, more effective, and better able to deal with the complex, cross-border issues the Internet comes with.

The Internet Society's *Multistakeholder Attributes* also provide an objective way to look at and continually improve our existing multistakeholder processes.

Multistakeholder is not a single model or 'all or nothing' solution. It is a way of doing things that can be used anywhere, from solving a specific problem or to helping an institution evolve.

Shared Goals and Methods

Goals

Both the OECD Security Guidelines and the experiences highlight how important shared goals are to success.

To sustain the open, distributed, and interconnected nature of the Internet – the key features integral to its success – we need to ensure policy decisions achieve the following:

- Maintain the security, stability, and resiliency of the Internet,
- Support global interoperability and an open and collaborative architecture,
- Sustain permission-less innovation and widening access, and
- Allow the Internet to flourish as a dynamic yet reliable platform for limitless opportunity and innovation around the world.

Methods

The global Internet community – people in almost every country from the technical community, business, civil society, and government – has over forty years of experience in creating, improving, deploying and coordinating the Internet. We have learned a lot about working effectively with and alongside a variety of legal and regulatory regimes.

Certain attributes should be applied to existing multistakeholder processes to keep them evolving to effectively serve the global public good. They can also be applied to a range of governmental and multilateral processes and institutions where they will help make decision-making more collaborative and effective, and produce workable outcomes that all stakeholders can implement:

1. **Inclusiveness and transparency,**
2. **Collective responsibility,**
3. **Effective decision-making and implementation, and**
4. **Collaboration through distributed and interoperable governance.**

MS IN ACTION

NETmundial

The NETmundial conference was held in São Paulo, Brazil, in April 2014, where it brought together 1,480 stakeholders from 97 countries. Working from over 180 written contributions from stakeholders around the world, NETmundial developed its Internet Governance Process Principles to guide the evolution of Internet cooperation and governance.

INTERNET GOVERNANCE PROCESS PRINCIPLES

Multistakeholder processes with meaningful and accountable participation, and roles and responsibilities of stakeholders flexible to the issue at hand

Open, participative, with consensus-driven decision-making where possible

Transparent, accountable, inclusive and equitable with bottom-up decision-making that doesn't disadvantage any category of stakeholder

Distributed and collaborative, a decentralized and multistakeholder ecosystem that encourages collaborative and cooperative approaches

Enabling meaningful participation where anyone affected by an issue can take part in decision-making, with capacity-building support if needed

Crucially, all these tools of multistakeholder decision-making were put at the service of a single, shared goal:

Internet governance should promote universal, equal opportunity, affordable and high quality Internet access so it can be an effective tool for enabling human development and social inclusion.

Multistakeholder Governance Attributes

Inclusiveness and transparency

Inclusiveness is the basis of legitimacy in collaborative decision-making. Those significantly affected by a decision should have the chance to be involved in making it. Inclusiveness is not just an admirable goal, but an essential part of an effective process. The less inclusive a process is, the less likely it is to engender the trust and support of those outside of the process. Transparency is an essential condition for inclusiveness, as it brings expert and affected groups into the process.

Transparency of inputs, process, and decision-making is fundamental to the Internet. The global technical community has long practiced a publicly archived process for developing technical standards. Our experience shows that secrecy, while sometimes necessary, is far less critical to effective decision-making than the greater range and quality of inputs. Transparency is also essential legitimacy as it can document that all stakeholders were heard.

Answering the following questions can help to assess and improve this requirement:

- *Do those significantly affected by a decision-making process have a chance to be involved in it?*
- *What practical barriers to entry exist – language, cost of participation, technical and process knowledge, cultural norms? Are there activities, processes, or alternative routes to mitigating them?*
- *What formal barriers to entry exist – membership criteria and restrictions – and are they absolutely necessary? What alternatives exist to widen participation and include more voices?*
- *Do all stakeholders have a shared understanding of the importance of transparency to inclusion, legitimacy, participation, and quality of output?*
- *Are all stakeholders committed to being as transparent as possible at all times – across inputs, process, and outputs – and documenting when and why transparency is not possible?*

Collective responsibility

All stakeholders share collective responsibility for the continued vitality of the Internet and the benefits it brings our societies and the global economy. In the technical community, we share a sense of collective stewardship of the Internet and the open standards its technologies are based on.

- *Do all stakeholders share a sense of collective responsibility, in their respective roles, for the future development of the Internet? Do they share the same goals of stewardship of a global public good?*

Effective decision-making and implementation

The most effective decisions are those based on an open and deliberative process that consider a broad range of information sources and perspectives. This holds for both the quality and implementation of the decision.

As the Internet is operated by a variety of public and private sector and civil society stakeholders, successful implementation of decisions needs imaginative and collaborative solutions. It is not as straightforward as passing a national law. Stakeholders who have been part of the process work harder to make its implementation a success.

International technical standards have typically relied on the voluntary adoption principle; they are chosen and defined based on technical merit, and applied according to their usefulness. In deliberating on issues of global Internet governance, we should ask:

- *Before the substantive discussions begin, does everyone agree on shared goals to guide the process and ensure the core questions are not debated multiple times?*

- *Is it clear from the outset – when shared goals are defined – that an outcome can feasibly be implemented by all relevant stakeholders?*
- *Is there a common understanding across stakeholder groups about how decisions will be made?*
- *Has everything been done to ensure that those who operate the infrastructure or are most affected by this decision have been part of making it? Has the process been sufficiently inclusive and transparent to maximise the ease of implementation?*

Collaboration through distributed and interoperable governance

Collaboration is the process of two or more people or institutions coming together to achieve a common goal. The Internet is the outcome of the collaborative efforts of different actors. It benefits from an increasing amount of actors teaming up and working together.

To effectively harness the efforts of many actors, the technical community has evolved autonomous governance systems based on collaboration and mutual respect. This means the organisations that coordinate the Internet can collaborate where needed and otherwise focus on doing their best at their respective jobs. The many organisations involved in Internet governance have complementary roles to play. We need to recognise this autonomy and keep dialogue and mutual participation in areas of overlap between organisations. This is how to keep our distributed global governance system fully interoperable.

- *Have we identified other processes or organisations also working in this space, and connected with them to share information and open dialogue? Are we committed to respecting the roles of other processes or organisations and being constructive and open-minded about using their outputs?*
- *In deliberating and making decisions, have we identified all stakeholders and collaborated with any interested or affected party?*
- *Have the right tools been used so stakeholders can scale up creative conversations and make connections organically?*
- *Are we open to sharing our findings and adopting the best working practices of other processes or organisations to keep improving?*

For more information and resources

Please go to **www.internetsociety.org/what-we-do/internet-issues/internet-governance**

Internet Society
Galerie Jean-Malbuisson 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

1775 Wiehle Ave. Suite 201
Reston, VA 20190, USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

www.internetsociety.org
info@isoc.org