Response to IGF BPF on Cybersecurity Open Consultation

Introduction

The WSIS Coalition is grateful for the opportunity to contribute to the Internet Governance Forum (IGF) Best Practice Forum (BPF) Open Consultation on Cybersecurity Culture, Norms and Values. We believe the input document compiled by the community is a valuable resource that can help drive forward the discussion of cybersecurity in the IGF context. As individual member companies, we all highly value our participation in the IGF and support the multistakeholder governance model at its core.

1. How do you define a culture of cybersecurity?
   a. We define a culture of cybersecurity as an overall awareness of cybersecurity risks, as well as a spirit of collaboration among the stakeholder groups involved in a community - users, the technical community, industry, and government - to identify opportunities and strategies to mitigate them. Attaining such a culture will enable a holistic approach that will enrich the dialogue around cybersecurity and help all stakeholders contribute in the most productive ways.

2. What are typical values and norms that are important to you or your constituents?
   a. For our customers, norms for cybersecurity are very important because they promote stability and increase the trustworthiness of the digital infrastructure they depend on for their livelihoods and economic advancement. To that end, we value and welcome norms that provide positive responsibilities for states and other actors to abide by that would positively impact their cybersecurity. A good example of such a norm is found in the 2015 report of the UNGGE, paragraph 13 (g), which states: "States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions." The protection of critical information infrastructure can improve the reliability of digital systems as well as have real-world consequences (such as keeping power grids and emergency communications networks online). This can help users further engage in the digital transformation of their communities, which will unlock their potential and foster social and economic development.

      We are also keenly interested in the development of cybersecurity norms in other venues which may be better suited to discussions of norms related to issues that are not solely inter-state ones. For example, the development of norms by the Global Commission for Stability in Cyberspace has captured important dynamics in the way that all stakeholders are involved in the protection of the public core of the Internet and in electoral systems. Because these critical components to modern life run on networks that are often owned and operated by the private sector, an approach that includes multi-stakeholder input and promotes collaboration between all relevant actors is better suited to their discussion.

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.
    a. The field of cybersecurity norms is relatively unique in that the makeup of norms authoring organizations reflects the diverse set of global stakeholders involved in the development of cyberspace itself: academia, the technical community, industry, users, and governments have all contributed to the discussion around norms, from within their various and respective areas of expertise. Industry has had a leading voice in the development of norms, leveraging our global visibility into the actions of harmful actors on the networks we operate to identify areas where international cooperation and agreement can be most impactful.

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?
    a. While the development of norms in cybersecurity is a relatively new environment, there are other areas of security where norms have been largely successful. We believe that there are useful parallels between the chemical and biological weapons discussion and the cybersecurity one. In particular, we believe there are lessons that our community can learn from the relative success of the use of norms in restricting the use of chemical and biological weapons. This successful creation, promotion, and adoption of norms restricting this devastating type of warfare has saved millions of lives and untold suffering. While there have been instances where norms have been broken, there is good evidence that most states abided by these norms, especially when they had confidence that other states would do so as well. Much like the cybersecurity landscape, the chemical and biological warfare arena also has dual-use technologies (lifesaving vaccines, for example) and a strong mix of academic, technical, and industry stakeholders supporting governments.

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?
    a. Norms are not always successful. Indeed, Finnemore (2017)[1] suggests that failure may be the most likely outcome for any given norm. One key element that could precipitate the failure of a norm is the lack of adaptability to meet new technological, cultural, and political realities. This could cause actors to abandon the norm out of convenience more than malicious intent and may lead to unintended consequences. It is therefore imperative that the hard work that goes in to development of norms create flexible norms that can be evolved over time.

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?
    a. While the development of cybersecurity norms is still relatively nascent (with the first truly global norms having appeared within the last 5 years), it is too early to tell whether the implementation of a given norm has been successful. Norms generally take long periods of time to achieve relative adherence, and violations of norms in other areas do occur, although rarely. We appear to still be in the "entrepreneurial" phase of norms development as defined by

[1] Finnemore M (2017), "Cybersecurity and the Concept of Norms," Carnegie Endowment for International Peace. Available at: http://carnegieendowment.org/2017/11/30/cybersecurity-and-concept-of-norms-pub-74870

Finnemore and Sikkink (2007)[2] and mass adoption has not yet materialized. However, we believe that the development of norms in the global context is important, as the security threats to the stability of the Internet are also global. There are, however, useful opportunities for the adoption of norms in the regional context. We are encouraged by Singapore's decision to promote the cyber norms agreed to within the UN Group of Governmental Experts (UNGGE) in 2015 within the context of the Association of South East Asian Nations (ASEAN) and hope that other countries in the region will support this initiative. In addition, the development of norms must be accompanied by the development of confidence-building measures and capacity-building programs to help states and other relevant actors understand how the norm is being adhered to by other actors and to internalize the norm into the actors' own processes and policies. This will be key to ensure national cybersecurity strategies are aligned with the values and objectives of the wider cybersecurity community, which will contribute to creating a safer cyberspace for all.

7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

   From our perspective, which allows us to view Internet developments in most countries, we see unequal opportunities for the application of security, which is concerning to our companies. We believe that in some countries, policy decisions can exacerbate these divides: forcing personal data to be localized in less secure systems that can't take advantage of the state of the art in cybersecurity, for example, can mean that users in some countries are forced to exist with a less-secure Internet experience, which can reduce their adoption of digital technology due to a lack of trust. Many online service providers have increasingly embraced security tools such as multi-factor authentication, making them available to users in all jurisdictions. The trend towards multi-factor authentication (and stronger forms of it) is positive for all users, and improves the overall security of the Internet. Given that the achievement of the Sustainable Development Goals (SDGs) will depend in great measure on the adoption of digital technologies, the stakes are very high. Decisions by national governments that do not consider the global nature of the cyberspace or take advantage of the global community's knowledge, expertise and development of best practices on cybersecurity can put users at risk. The same goes for governments that adopt policies that do not foster collaboration between stakeholders both within and across their borders in terms of digital skills training and cybersecurity awareness raising.

About the WSIS Coalition

The WSIS Coalition represents major global ICT companies involved in many aspects of the Internet ecosystem. We are strong supporters of the multi-stakeholder model for policy development and seek to promote the goals of the World Summit on the Information Society (WSIS). We are dedicated to the continued development of a global open, secure, and interoperable Internet to foster social and economic development for all people.

[2] Finnemore M and Sikkink K, (2007), "International Norm Dynamics and Political Change," International Organization, Vol. 52, No. 4, International Organization at Fifty: Exploration and Contestation in the Study of World Politics. (Autumn, 1998), pp. 887-917. Available at: http://links.jstor.org/sici?sici=0020-8183%28199823%2952%3A4%3C887%3AINDAPC%3E2.0.CO%3B2-M