Freedom Online Coalition Working Group 1 "An Internet Free and Secure"

Submission to the IGF BPF on Cybersecurity

Question:

What are the typical roles and responsibilities of your/each of the stakeholder groups in making the internet a secure and safe place for people to socialize and conduct business?

The roles and responsibilities of stakeholders are evolving in making the Internet a secure and safe place for people to socialize and conduct business. It is clear that security is no longer just the purview of governments and that it is increasingly a multistakeholder imperative. With cybersecurity and cybercrime challenges increasing in frequency and complexity there is a need for all stakeholders to work together to address these in a manner that preserves human rights, particularly privacy and free expression.

The call for cybersecurity policies to be developed in a more open and inclusive manner with greater protections for human rights has been growing:

> The Seoul Framework that resulted from the Seoul meeting of the London Process in 2013 states that it is "necessary to continue to work together towards ensuring a trusted, secure and sustainable environment in partnership with multiple stakeholders, including international organizations and the private sector."
>
> The 2014 NETMundial Multistakeholder Statement noted, inter alia, that "initiatives to improve cybersecurity and address digital security threats should involve appropriate collaboration among governments, private sector, civil society, academia and technical community."
>
> And, the Chair's statement at the 2015 GCCS meeting in The Hague urged governments "to ensure that cyber policy at national, regional and international level is developed through multistakeholder approaches, including civil society, the technical community, businesses and governments across the globe."

Despite the recognition that cyber issues should be dealt with involving all stakeholders, there are few fora in which cybersecurity related concerns can be discussed on a multistakeholder basis. Various issue specific meetings may be held on cybersecurity

matters to which other stakeholders are involved, but the degree to which civil society are engaged and welcomed is minimal, particularly in cybersecurity policy and norm-setting processes. Much work remains to be done to realize and put into practice the increasing calls for multistakeholder approaches – now is the time for all stakeholders to work together to make this a reality.

The Freedom Online Coalition Working Group 1 on "An internet Free and Secure" has undertaken the following mapping of cyber security spaces and processes which assesses the degree to which they are open or not to stakeholders: https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/Mapping-Brochure-WEB-1.pdf This mapping exercise clearly illustrated the degree to which cybersecurity processes and fora remain closed to stakeholders and particularly civil society. For more on FOC WG1 see below.

Questions:

What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?

What are some examples of best practices in 'Cyber security Situational Awareness' where different organizations have worked together, specifically with law enforcement agencies and other specialists?

The Freedom Online Coalition Working Group 1 - "An Internet Free and Secure" (FOC WG1) is a notable and highly functioning example of multistakeholder collaboration on cybersecurity. The purpose of FOC WG1 has been to bring a human rights framing to ongoing cybersecurity debates. It aims to develop, through multistakeholder dialogue, meaningful outputs that feed into existing cybersecurity processes and the creation of new, more effective, human rights enhancing cybersecurity policy.

The Working Group's purpose, composition and blog series can be found here:

https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/

The Terms of Reference for the Working Group can be found here:

https://www.freedomonlinecoalition.com/wp-content/uploads/2015/07/FOC-WG-TOR-FINAL-July-13--2015.pdf

The WG was created as a multistakeholder exercise by design, noting UNGA Resolution 57/239 on the creation of a global culture of cybersecurity and in particular the Annex on

Elements for creating a global culture of cybersecurity notes the importance of stakeholders working together.

FOC-WG 1 can serve as a model for successful multistakeholder collaboration on cyber security between private sector, civil society and governments. The work involved Internet policy, cybersecurity and governance experts from across stakeholder groupings, was driven by collaborative and open dialogue and resulted in multiple significant outputs. Notably, the WG has developed the following:

A definition of cybersecurity focussed on information and individual security:

https://www.freedomonlinecoalition.com/how-we-work/working-groups/working-group-1/blog8/

In order to advance the normative debate on cybersecurity, the WG developed a set of recommendations that promote greater stakeholder-driven and human rights respecting approaches to cybersecurity. These recommendations were developed with the aim to provide guidance to all stakeholders involved in cybersecurity matters, and in particular those involved in developing and implementing cybersecurity policies and frameworks. They are designed to encourage stakeholders to incorporate the protection and promotion of human rights in all matters related to cybersecurity and to ensure that cybersecurity policy is rights-respecting by design:

https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Recommendations-Final-21Sept-2015.pdf

A backgrounder to the recommendations that outlines the need for a paradigm shift in the way that stakeholders address human rights and cybersecurity was also produced:

https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-WG1-Narrative-Final-28-April-2016.pdf

And, as a step towards facilitating greater stakeholder engagement in cybersecurity debates, the working group conducted a mapping exercise to identify main global spaces where cybersecurity is being discussed. The main objective of this exercise was to raise awareness among the broader community. The final output of the exercise was a visual timeline of relevant global spaces where cybersecurity debates are taking place:

https://www.freedomonlinecoalition.com/wp-content/uploads/2015/05/Mapping-Brochure-WEB-1.pdf

In the public debate about how to provide security in the digital context, the dominant narrative has become increasingly entrenched pitting privacy and other human rights

against public safety and national security. In practice, though, threats to privacy and other human rights can also harm public safety and security. This binary framing is therefore damaging to both sides of the equation, and creates antagonisms where mutual reinforcement is possible. Framing privacy and other human rights as antithetical to public safety and national security is not only misleading, but undermines public safety and security, as well as freedom. Raising the profile of human rights protections in existing cybersecurity policy-making is necessary to offset this trend.

These recommendations are a first step towards ensuring that cybersecurity policies and practices are based upon and fully consistent with human rights – that cyber security policies are rights respecting by design.

These recommendations were shared with the community in a successful workshop at the IGF in Brazil in 2015, the report for which can be found here: https://www.intgovforum.org/cms/wks2015/index.php/proposal/view_public/186

The recommendations were also the subject of a session at RightsCon in March of 2016, the video for which can be found here: https://www.youtube.com/watch?v=3IhlNEdpOks&index=10&list=PLprTandRM961m3pHsOlfij8wd9C_PHgqm

The final version of the recommendations will be presented at the 2016 annual meeting of the FOC meeting in Costa Rica October 16th and 17th.