STRENGTHENING THE MULTI-STAKEHOLDER APPROACH TO NORMS IN CYBERSPACE

DAY-0 WORKSHOP REPORT

Internet Governance Forum 25 November 2019, 10:35-12:35
Berlin, Germany

Methodology

The international discussion on norms of acceptable behaviour of states in cyberspace has been prominent on the international agenda as cyberspace increasingly became an area of strategic concern. As obligations and duties under international law primarily apply to states, the United Nations forms a primary avenue to formulate norms of responsible state behaviour in cyberspace. Norm-construction efforts have also been undertaken by non-state actors, especially after the perceived 'failure' of the 2017 UNGGE, resulting in several norm-building initiatives and a flourishing norms entrepreneurship. In 2019 another UN Group of Governmental Experts (UNGGE) and an Open-Ended Working Group (OEWG) was instigated to continue the discussion on responsible behaviour in cyberspace. An intersessional stakeholder meeting of the OEWG was proposed 'with a view to making the United Nations negotiation process on security in the use of information and communications technologies more democratic, inclusive and transparent'.

The evolution of international norms construction demonstrates an increasing interest for broader participation and collaboration among governments, private sector, civil society, academia and technical community. While states remain the duty bearers for human rights and security, non-governmental stakeholders have a role to play in cyber norms cultivation.[1] Non-governmental stakeholders play an essential part in implementing solutions, but the respective roles and responsibilities of stakeholders in this process are not set in stone. Rather, they are interpreted in a flexible manner depending on the issue under discussion. As described by Finnemore, the three stages of norms cultivation are: norms articulation and promulgation; norm dissemination; and norm

[1] Eggenschwiler, Jacqueline (2019) *International Cybersecurity Norm Development*, https://eucyberdirect.eu/content_research/1064/

internalization, institutionalization and enforcement.[2] As norms are constantly in transition, it is imperative that stakeholders take up a role in all parts of norms cultivation.

The following roles can guide stakeholders in this participation:[3]

- **Stakeholders as problem-solvers**

Problem solving is the most obvious role for non-governmental stakeholders, as the ICT infrastructure is mostly in the hands of private companies, the technical community secures the infrastructure, civil society has the reach to improve resilience in society and academia and experts have the knowledge and expertise to develop solutions. Facilitating norm internalization for stakeholders is however only possible for non-governmental actors if they are given the right mandate and resources.

- **Stakeholders as opinion-shapers**

A diversity of perspectives is needed in the establishment of a norm. Non-governmental stakeholders can shape opinion and perspectives and engage with states when they articulate and institutionalize a norm, making the norm more inclusive and supported by a broader layer of society, providing it with more democratic legitimacy. Debates in and between stakeholder groups also contribute to promulgation, dissemination and internalization of a norm.

- **Stakeholders as community-builders**

Building community within one's own stakeholder group facilitates the dissemination of a norm, and unites support to internalize a norm. A strong community with a consultation process can also form more nuanced suggestions for the modification of a norm or when contesting a norm. Non-governmental stakeholders can also bridge communities and build trust to facilitate communication. This is imperative for all steps of norm cultivation.

- **Stakeholders as decision-makers**

States still have the monopoly of power to stipulate red-lines, and are thus the prime rule-makers in a state-based international system. Non-governmental stakeholders however have a role to play in providing expertise when norms are internalized through law, or institutionalized and enforced through policy. They also have the power through democratic processes to put pressure on their decision makers if decisions do not respect stakeholder interests and benefit society.

- **Stakeholders as whistle-blowers**

Enforcement belongs to the realm of states, but non-governmental stakeholders can monitor the adherence to a norm by spreading awareness on its violation. They can put pressure on enforcement by whistleblowing and regular reporting.

Internet Governance Forum Day-Zero workshop

Participants from civil society, academia, the technical community, private sector and governments were asked to reflect on their roles, and make recommendations on overcoming challenges when fulfilling different roles. The workshop had the following objectives:

---

[2] Finnemore, Martha (2011) *Cultivating International Cyber Norms*, https://citizenlab.org/cybernorms2011/cultivating.pdf

[3] Lété, Bruno (2019) *Shaping Inclusive Governance in Cyberspace*, German Marshall Fund http://www.gmfus.org/publications/shaping-inclusive-governance-cyberspace

- Building awareness on stakeholders' involvement in the international development of norms on responsible state behaviour
- Stimulating a reflection on roles and how specific actions of stakeholders contribute to the implementation of norms
- Stimulating an exchange on best practices between different stakeholders in taking actions in particular roles.
- Providing support between stakeholders on overcoming challenges in fulfilling different roles.

The annex to this report describes the workshop methods and resulting conclusions of discussion.

ANNEX

Workshop Method

Participants were divided into 4 groups according to 4 UNGGE norms:

- "States should encourage **responsible reporting of ICT vulnerabilities** and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT dependent infrastructure"
- "States, in ensuring the secure use of ICTs, should **respect Human Rights Council resolutions 20/8 and 26/13** on the promotion, protection and enjoyment of human rights on the Internet, as well as **General Assembly resolutions 68/167 and 69/166** on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression"
- "States should take reasonable steps to **ensure the integrity of the supply chain** so that end users can have confidence in the security of ICT products. States should see to **prevent the proliferation of malicious ICT tools and techniques** and the use of harmful hidden functions."
- "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"

Participants were asked to reflect on their role as opinion-shapers, community-builders, decision makers, problem-solvers and whistleblowers for a specific norm. They were encouraged to write down which specific actions they've undertaken in every role. They were then asked which challenges they face in different roles. The first half of the workshop focused on exchanging experiences and mapping the possible actions per role for different stakeholders. The second half of the workshop discussed how to overcome certain challenges. Following questions guided the discussion:

- Which actions overcame another stakeholder's challenge, and how did the stakeholder do this?
- What is needed to overcome other challenges?
- Does everyone in this stakeholder group and outside of this stakeholder group encounter these challenges?

- How can your stakeholder group assist another with a certain challenge?

Conclusions

1. What became clear is that there is a lot of involvement of all stakeholders in opinion shaping around all of the norms, but there is a disconnect in understanding from policymakers and the general public. Some stakeholders noted they have become more aware of the need for a translation exercise and advised others who struggled with a similar challenge.
2. There did not appear to be much collaboration with governmental stakeholders on problem solving and decision making, most stakeholders worked in a multi-stakeholder approach without much government involvement and some created rules for their own organisations.
3. A recurring challenge for all stakeholders across all norms to do norm monitoring was a lack of information and oversight. This was strongest among stakeholders who didn't fill the role of community-building well.
4. Exchanges on community-building were identified as one of the priorities, as the efforts are very fragmented and unnecessarily duplicated. A culture shift is needed to allow and empower non-governmental stakeholders to take the lead in uniting these efforts, as well as provide the resources, and for governmental stakeholders to be more present in spaces where community is being built, such as at the IGF.

Group I: Reporting ICT vulnerabilities

Moderated by Laura Groenendaal - German Marshall Fund

1. Participants found that policymakers don't really understand how the internet works, making it difficult for the technical community to talk to policymakers and influence opinion.

2. Companies have a hard time allowing other stakeholders to fulfil a role, especially on observation of the norm to report vulnerabilities, the conflict of interest remains the main challenge.

3. Participants added that the norm needs to be complemented with an obligation to implement a secure development lifecycle, which is the root cause. This norms should also go hand in hand with the norm on protecting the supply chain, and the prohibition that vulnerabilities should not be stockpiled. The biggest challenge in this is a lack of information and openness. The Vulnerability equities processes are a step in the right direction.

Participants

- JPCERT (technical community)
- CERT.BR (technical community)
- CERT.BR (technical community)
- UCSD (academia)
- NCC Group (private sector)
- CIRA (ccTLD Canada) (technical community)
- CMU – IEEE (technical community)

Group II: Human rights

Moderated by Kate Saslow - Stiftung Neue Verantwortung e.V.

1. Stakeholders noticed they already take up many roles, many actions are being taken by human rights organisations as they are very developed in this space.

2. There are some stakeholders, especially in the private sector, working more on providing evidence to see the impact of measures, and creating their own legislation in the face of a lack of legislation from governments, to protect human rights.

3. One of the main challenges for problem solving is a lack of coherence in international law, international principles and national rule of law, especially for the private sector. Participants initially wondered how the UNGGE norms are related to other human rights provisions and mechanisms.

Participants

- Facebook (Private sector)
- African Union commission (PRIDA) (Government)
- Reporters without Borders (civil society)
- Viakult Office/KidsFast (civil society)
- The Arab Center for the advancement of social media (civil society)
- Global Partners Digital (civil society)
- Hamburg University (academia)
- Together Against Cybercrime (civil society)
- US Patent and Trademark Office (technical community)
- NIC.Brasil (technical community)
- Asociacion por los derechos civiles (Civil society)

Group III: Protecting Critical infrastructure

Moderated by Bruno Lété - German Marshall Fund

1. Government stakeholders noted there are several opportunities for opinion-shaping and decision-making but not everyone makes use of public consultations and existing platforms.
2. Non-governmental participants noted that to create norms observation and whistleblowing, there needs to be a legal protection and procedures to follow up the risk.
3. The problem for any participation in observing the norm on protecting critical infrastructure is the low availability of information, which needs to be secretive for legitimate reasons. This also means it's hard to have an informed discussion with other stakeholders as they cannot have an insider view.

Participants

- Microsoft (private sector)
- JPRS Japan (technical community)
- Canadian MFA (government)
- Portuguese MFA (government)

- World Trade Organisation (Intergovernmental)
- Ukranian civil society
- Caribean government
- Subsahel government
- African legal academic

Group IV: Supply chain security

Moderated by Julia Schuetze, Stiftung Neue Verantwortung e.V.

1. Making consumers aware of online security and making governmental stakeholders conscious about security decisions is challenging because of the technical complexity. Some participants had more experience communicating with these groups than others.

2. Creating a Vulnerability Equities Process needs to be implemented by governmental stakeholders, but other stakeholders have created trusted processes in their own systems and make their own rules, therefore taking the lead on rule-making.

3. Multistakeholder formats are important to build relationships with communities who can work on problem solving but there is not enough investment. The lack of resources makes it hard to create rules and assess risks.

Participants

- Internet Society (Technical community)
- NEC (private sector)
- ICC (private sector)
- Private sector
- Civil society
- Civil society
- Academia