3 May 2021

Digital Coffee Meeting

Memo by Anthony Rosborough

"Cyber capacity building in the Global South: A model for overcoming inequalities in transnational governance?"

Speaker: Dr. Andrea Calderaro (EUI and Cardiff University)

This event has been organised by the Technological Change and Society Interdisciplinary Research Cluster

The Digital Coffee Meetings are informal meetings which involve brief presentations regarding digital transition intended to be delivered in non-technical and jargon-free language. Digital Coffee Meetings are intended to facilitate knowledge sharing among members of the EUI community. Dr. Calderaro is a Visiting Fellow at the EUI and Senior Lecturer in International Relations at Cardiff University. His talk addressed cyber capacity building in the Global South and why the capacity of developing states to have robust cyber capabilities and infrastructure is of interest to the entire world.

Dr. Calderaro began his talk with a series of questions - why should we care about cyber capacity building at all? What does cyber capacity building mean? What are the current and future challenges in this field? In response, Dr. Calderaro reminded attendees of the transnational nature of the internet. It is made of data centres, servers, and all of which are connected through physical cables. The backbone of this network is an array of submarine fiber optic cables. This results inevitable geopolitical debates that underpin the functioning of the internet, including occasional tensions and negotiations. Dr. Calderaro drew attention to the fact that submarine cables present interesting geopolitical issues because they are strewn across the ocean bottom in areas beyond the national jurisdiction of any state. As a result, they are built and managed by a handful of private companies in the telecommunications sector. Dr. Calderaro stressed that this physical presence of the internet and its concentrated governance regime is crucial for our understanding of cyber capability building because any new initiatives need to cooperate with industry. Adding to this dynamic, Dr. Calderaro noted that states and individual users have very little control over the routing of data, that functions beyond national legislations.

As a result of this, there is an increasing need to strengthen a Transnational Governance Approach to the cyber domain. With this in mind, Dr. Calderaro sought to focus the attention of his talk toward *security* and what exactly means to enhance a Transnational Governance approach in the context of safety and security of the cyber domain.

Under the banner of 'cyber security' we have witnessed a proliferation of national frameworks and initiatives. But given the transnational nature of the internet, in addition to national efforts, we are witnessing an increasing call to strengthen international cooperation in the cyber domain, giving live to a so-called 'Cyberdiplomacy'. This call has been translated by the UN into the UN Group of Governmental Experts (UNGGE) and the Open-Ended Working Groups (UNOEWG). These are two complimentary committees aiming at negotiating what safety and security in the cyber domain means and to release the first UN Treaty on Cyber Security. The UN Group of Governmental Experts includes only 25 members, where the UN Open-Ended Groups involve all remaining UN members, and other non-state actors, including members of industry and civil society. While the UNOEWG has already agreed on a final resolution approved by consensus in March 2021, Dr. Calderaro anticipated that the preliminary documentation negotiated by the UNGGE for the creation of this Treaty is supposed to be released in June 2021, if all goes according to plans.

Truly global, transnational, and multistakeholder governance approach to international cooperation in the cyber domain is essential. As Dr. Calderaro remarked, most of today's internet users are not in the Global North anymore. Safety and security of the internet, therefore, requires a more globally representative approach to be legitimate, beyond the Global North. Now that the Digital Divide has narrowed, the currently experienced Digital Transformation in the Global South should be supported with cyber capacity building strategies. given this emerging priority, the UN's efforts have therefore worked toward this as a key priority. And this is also reflected in the European Union's "Operational Guidance for the EU's International Cooperation on Cyber Capacity Building".

Given the experience gained over the last years, what could be done better? Dr. Calderaro asked. Most of the strategies have been focused primarily on the ambiguity of "capacity building". Who ought to work toward increasing this capacity? States, private industry, international organisations? Which community within states needs to develop this capacity? What is the subject of this capacity, state security, human rights, economy?

In response, Dr. Calderaro opined that cyber security is not merely the responsibility of the state, but also of industry as the owner of the infrastructure. It is also the responsibility of civil society, as citizens are the main targets of cyber-attacks. This means that cyber capacity building efforts needs to be diversified, depending on which stakeholders are the target of these. Yet, the concept of 'cyber' needs also to be approached more holistically, beyond security concerns. Dr. Calderaro put forward a definition of cyber capacity building as:

"The diffusion of technical, governance and diplomatic skills among relevant stakeholders, including government, industry and civil society actors, to ensure the development of sustainable connectivity". [1]

In attempting to reach international consensus on this concept, Dr. Calderaro remarked that the bulk of the submissions to the UN OEWG have so far come from actors in the Global North. States in the Global South have not been particularly active, and Africa in particular has been almost entirely missing from the discussion. Given the need to strengthen an inclusive Transnational Governance approach to the Cyber Domain, Dr. Calderaro stressed the importance of empowering the Global South to develop their cyber diplomatic capacity in order to have a say on how the functioning digital technologies could reflect their own socio-political and economic contexts.

A EUI researcher asked Dr. Calderaro whether efforts at the UN level has so far been targeted at addressing existing international treaties which may result in an inability for states to increase cyber capacity. He referred to the United Nations Convention on the Law of the Sea, which leaves a regulatory gap in the case of submarine cables on the high seas which can be subject to intentional damage or attack. Dr. Calderaro confirmed that the revision of existing treaties has not yet been part of the discussions at the UN level. Rather, the discussions so far have been focused at establishing general principles.

Overall, Dr. Calderaro's talk shed light upon an aspect of digital regulation that often goes unnoticed. Namely, the physical nature of the internet as a series of fiber optic cables, and the role of state regulating in protecting its integrity. It remains to be seen whether participation from the states in the Global South will strengthen in these discussions, or if such states with relatively undeveloped cyber capacity opt instead for a more fragmented approach.

[1] Calderaro, Andrea, and Anthony J. S. Craig. 2020. "Transnational Governance of Cybersecurity: Policy Challenges and Global Inequalities in Cyber Capacity Building." Third World Quarterly 41(6): 917–38.

If the latter approach is taken, Dr. Calderaro's talk reveals that the international community could be latter approach is taken, Dr. Calderaro's talk reveals that the international community could be much worse off. Efforts afoot at the UN level and within the European Union show promise toward the creation of global principles and norms to ensure the efficacy and security of the internet as a common economic and social resource for all.