meeting report

internet democracy project

Cybersecurity, Internet Governance & India's Foreign Policy: Antecedents and The Way Forward for Non-Governmental Stakeholders

INDIA HABITAT CENTRE, NEW DELHI, 27TH FEB 2016

On 27 February, 2016, the Internet Democracy Project organised a national meeting of non-governmental stakeholders at the India Habitat Centre in Delhi, to discuss the findings of its latest research study, 'Cybersecurity, Internet Governance and India's Foreign Policy: Historical Antecedents' by Mr. Saikat Datta.

The paper, commissioned as part of the Internet Democracy Project's work on cybersecurity and Internet governance, aims to contribute to a greater understanding of India's cybersecurity concerns and of the ways in which India approaches global Internet governance fora to address pressing issues.

The goal of the meeting was to discuss the implications of the paper's findings for non-government stakeholders in India in greater detail.

The meeting was a closed event, attended by a diverse set of invitees from civil society organisations, members of the technical community (such as ICANN), representatives of the start-up ecosystem, academics and journalists. It was held under the Chatham House rule.

1. Setting the scene

Dr. Anja Kovacs, Director of the Internet Democracy Project, kicked off the meeting by explaining the rationale for the research and the event. A few exceptions notwithstanding, the Indian government has generally assumed a dominant role for the State in formulating policies and building cooperation in cyberspace. For long, representatives of the Indian government were staunchly in favour of governments taking up an oversight function in global Internet governance.

This position changed when Union Minister for Communication and Information Technology, Ravi Shankar Prasad, announced, during the ICANN53 meeting in June 2015, that India would support a multistakeholder model of governance, in line with the position of countries such as the United States. In spite of shifting from a multilateral approach to supporting a multistakeholder model, however, the Indian state continues to engage with non-governmental stakeholders outside of the private sector only in a very limited manner.

Engagement on cybersecurity matters has proven to be particularly challenging, not in the least because of a trust deficit between the security community in the government, on the one hand, and non-governmental stakeholders like human rights advocates and technologists, on the other. The research conducted by Saikat for the Internet Democracy Project aims to start bridging that gap, by providing a better understanding of India's positions, their context and history. In this way, the research also hopes to contribute to strengthening ways and spaces for the different communities to engage.

2. The research and its findings

Saikat started the introduction of his research by explaining the economic moorings of India's foreign policy on technology. He pointed out the importance that modern technologies and engineering have played in moulding Indian hopes and ambitions as a leader of the modern world. At the same time, however, he explained, shifts in India's domestic economic policies have deeply impacted its foreign relations as well as its embrace of technology. Of particular importance was a shift from state-controlled economic policies to a new belief in opportunities for economic growth through the strengthening of bonds between state and private industry in the 1980s. This led to India's first telecommunication revolution and extensive computerisation, including of the railway ticketing system in 1987. The first crucial network that would need to be secure had thus been set up.

Saikat next went on to detail the long history of technology denial experienced by India, most acutely in its nuclear and space programs. He framed India's opposition to technology control regimes that impact on cybersecurity, like the Wassenaar Arrangement, against the background of these technology denial regimes. India's opposition to such regimes continued in 2013 when the list of dual-use technologies under the Wassenaar Arrangement was expanded to include 'intrusion software'.

Saikat then explained how the economic crisis in the early 1990s again led to a new course in foreign policy. Ties established with the United States in 2000-2001, especially, have been very strong and have influenced India's stances on cybersecurity since. He explained how India often uses bilateral negotiations to make up for its lack of a seat in multilateral arrangements that it is not part of, such as the Wassenaar Arrangement. He further highlighted how in more recent times, there is often a discrepancy between India's international stances, in which it now espouses multistakeholder models of Internet governance, and its policies nationally, where there is all-too-often blatant unilateral and non-consultative policy-making.

Saikat finally went on to illustrate how terrorism has been a driver of debates and cooperation around cybersecurity matters in India, ultimately steering India's global Internet governance positions. He also explained how the domestic framework for cybersecurity has, however, not kept sufficient pace with India's demands and positions abroad.

3. Feedback received earlier from government officials and other experts

On 12 February 2016, the Internet Democracy Project had co-organised, with the Observer Research Foundation, a meeting with senior government officials, practitioners, regulators and key members of the strategic community to allow them to respond to Saikat's paper and to facilitate further discussions. Anja next continued by flagging some key points and themes that had emerged from that meeting.

These included a broad agreement that, for India to emerge as a leader in the twenty first century, it would have to adapt its approach to foreign policy. But on what that would mean exactly, there was no consensus as yet. While there was general recognition that greater engagement with all stakeholders will be an essential element, some also expressed the sentiment that, in a democratic society, elected representatives of the government should have a leading role even in multistakeholder models of governance. Plenty of criticism was stacked against the United States, as its lack of support for multilateralism was correctly seen as convenient: at present, the multistakeholder system disproportionately benefits the US, which is far ahead of other countries in controlling domestic and global internet resources. India's often moralistic approach to foreign policy was also flagged as problematic, in that it often ends up harming the country's interests. Instead, a pragmatic approach, as well as building internal capacity in order to have negotiating power, were pegged as the need of the hour.

4. Open discussion

After flagging the above themes, it was noted that it is important for other stakeholder groups as well to think through these issues. Does multistakeholderism have value even where cybersecurity is concerned? And if yes, what does or should that mean in practice? With these questions, the discussion was opened.

There was general agreement that means for non-governmental stakeholders to engage in Internet governance and cybersecurity should be explored, and mechanisms should be created where existing ones are insufficient. One person pointed out that while security measures are undeniably important, good policy-making lies in balancing countervailing forces. For this reason, it is essential that all stakeholders are provided the opportunity to engage and get involved, including on cybersecurity issues.

One participant also pointed out the influence that India's laws and policies have on its neighbours (Bangladesh, Nepal, Sri Lanka and Pakistan), especially in emerging areas like governance of the Internet. For example, the Supreme Court judgment striking down Section 66A of the IT Act is influencing court decisions in Pakistan and Bangladesh. At the same time, neighbouring countries are also taking India's cue on Internet shutdowns under Section 144 of the Criminal Code of Procedure.

The rest of the discussion ensued around the following themes:

Insufficiency of current mechanisms like MAG: It was pointed out that the Indian Multistakeholder Advisory Group (MAG) as it stands is woefully lacking. It has been appointed in a top-down manner, doesn't meet often enough and does not function in a transparent manner. There have to be mechanisms for persons to meet often, and to channel inputs from a broad range of players in the private sector and civil society to feed into government models.

As it stands now, the private sector seems to have taken over the Indian nominations to the

global Multistakeholder Advisory Group.

Need for new institutional mechanisms of engagement: It was pointed out that while security considerations are important, every measure that mounts security as a priority that overrides other considerations should be compared with available alternatives. For example, in the aftermath of the revelations that terrorist outfits had used open wifi networks, the Department of Telecommunications came up with a notification that made anyone operating open wifi networks punishable. Strictly speaking, this brought within its sweep also persons who do not secure their wifi networks at home with a password. Moreover, signing in to free wifi networks offered at public spaces subsequently became a painful procedure, requiring multiple levels of authentication. Even in other highly security-conscious countries, such complicated procedures are not common. The process of signing in and authenticating with a phone number is a hindrance to what can otherwise be a simple experience.

What this example makes clear is that every decision has direct implications for users and businesses, and therefore it is crucial to consider carefully what the best security design is among available alternatives. If requiring users to sign in with a One-Time-Password is indeed the only way to ensure security, then it is acceptable. But there should be fora where discussions and positive exchanges on the viability of alternatives is possible. Concerns were also expressed that no consultations had been conducted with wider stakeholders about newly emerging bodies like the National Media Analytics Centre.

In addition, it was pointed out that there is also a need for lightweight institutional mechanisms of cooperation within the government, which should be able to easily accommodate the different departments and ministries of the government with roles in Internet governance, such as the Ministry of Home Affairs, the Department of Electronics and IT, the Ministry of Defence and others.

Indiginisation goals should include openness of participation: In the past, in the Indian private sector, IT companies have not been innovators: big businesses were mostly built on servicing the huge outsourcing industry. But this trend is fast changing. Indian companies are acquiring core technologies and this is indicative of a more ambitious moment. This turning point should be accompanied with greater engagement in matters of Internet governance and cybersecurity by the private sector, including by start-ups.

It was noted that the United States' influence in cyberspace (apart from being incumbents) can be put down to strong government participation combined with strong private sector and non-governmental participation from the country. In the near future, when Indian companies will be big, the stakes in India, too, will be higher and the number of stakeholders larger, and it is important to start pushing for spaces for wider engagement at the national level now. With India likely soon having the largest number of Internet users of any country, it is important to embed democratic participation in all evolving processes, and to make the most of a wide number of users by welcoming their contributions throughout.

Sense of distrust is a challenge: The Government believes that the private sector and civil society have vested interests, and in turn, civil society and the private sector do not trust the government. One participant offered that for a multistakeholder platform to work, trust is most

important. On some issues, at some points of a process, confidentiality is too. The government has to be certain that that confidentiality will be respected. When designing processes for multistakeholder participation, such concerns have to be taken into account if trust is to be fostered.

Extension of sovereignty: Many countries bring up Russia and China as examples of countries that guard their sovereignty closely when it comes to law-making and governance of the cyberspace, but, it was pointed, it is important to remember that all countries protect their sovereignty, including Westerns countries. In this context, one participant also wondered whether other stakeholders should perhaps accept state sovereignty as the much-needed meeting ground and give governments their 'due place'.

Non-governmental stakeholders ripe with capacity to be tapped: Despite projects like Digital India and e-governance and ICT for development projects, which encourage wide-scale public engagement and uptake of the Internet, there is very little room for stakeholders outside the government to, for example, engage and help build robustness of infrastructure in India. One participant noted that hackers, for instance, should be engaged and employed by the government as they have particular technical knowledge and capacity that is lacking within the government.

It was also noted that Indian civil society is well engaged by and large in Internet Governance issues, and has done a remarkable job in highlighting issues that are of domestic and international importance. This understanding and expertise can and should be utilised in a positive manner by the Government.

Multistakeholderism as a work-in-progress: It was pointed out that as a process of cooperation, multistakeholderism is less than 20 years old. In its initial years, the Internet was predominantly populated by English speaking countries, but it is going to look very different in the coming future. It is essential that space for geographic, linguistic and demographic diversity in Internet governance is ensured both at national and global level. While private sector participants will always easily find their way to these processes if these are in their interests, the participation of diverse other stakeholders requires proactive attention and support.

It was pointed out that the government feels the need to lead the multistakeholder process. Participants expressed a need for a structure that can accommodate a wide range of voices. In addition, it was noted, in a complex country like ours, there is a need not only for institution building, but also for capacity building for multistakeholder processes to work. It is important for us to recognise the value of existing systems, like the standards building processes within ICANN etc., and see the use for these. One participant pointed out that the current conversation about multistakeholderism is still about inside-power and not wider public participation, and that there is a need to cast the net wider. A multitude of processes might be needed.

Capacity building within and outside the government: Important plugs to address include capacity building for the government, and capacity utilisation by the government. It was pointed out that just like many economic or financial policy think-tanks are quite

sophisticated, there is a need for independent policy bodies on Internet governance that the government trusts, but that also produce world class reports. The cyber realm is as important as the financial realm, and there is a need for many to provide inputs. Professional input to the government in this area is important.

It was also noted that a large part of research on Internet governance related issues is conducted only as and when the issue in question becomes of immediate importance. It is important, however, to also start conducting long-term studies on many of the questions raised, such as the trade-offs between net neutrality and affordable access in free market models.

In addition, it was pointed out that while we keep an eye on how domestic stances reflect in the international space, it is equally important to keep an eye on the international developments that will affect Indian cyberspace and to actively participate in shaping those. Processes like those in ICANN, the International Telecommunications Union (ITU), etc. are important fora to represent the interests of different stakeholder groups, including disadvantaged groups and minorities.

Finally, it was noted that many university departments that study foreign policy continue to restrict themselves to traditional bilateral and multilateral forms of cooperation. Addressing complex and nascent foreign policy matters like multistakeholder cooperation is very important. There is a need to popularise the understanding of the politics of cyberspace, so that there can be wider public engagement and interest on these issues. The need for a cooperative spirit among civil society actors was pointed out.

5. Final remarks

To close the meeting, Saikat and Anja answered some questions that had been directed specifically at them.

In response to questions about handling terrorist outfits and the role of non-government stakeholders in this, Saikat pointed out that this is the age of ‘franchise terrorism’, in which people with different capacities come together to attack when needed. In this way, outfits like ISIS can work beyond their territorial boundaries and strength in numbers. The same is needed to counter them.

Saikat, thus, stressed on working with teams that include a variety of capacities, as the intermingling of disciplines can be of enormous value – the skills and perspectives of the intelligence community, activists, start-up founders, journalists, designers, etc. are unique, and when brought together, they can be utilised in reinforcing ways. For many problems, the government is still looking to bilateral engagement with other countries for solutions, rather than tapping into the capacity that is available locally, albeit outside of government or bilateral mechanisms. He said that more engagement begets more intelligence; a reluctance to engage is crippling any intelligence gathering.

Anja commented that bilateral engagement on issues of cybersecurity has certainly increased

over the past eight months or so, and this makes sense from the state's perspective, but from the perspective of other stakeholders, it is worrisome. She pointed out that for bilateral engagements, one needs to be invited into the room in order to be able to take part.

Finally, both also made some closing remarks. Saikat, commenting generally on the discussion, said that using 'security' is not a good enough reason for exclusionary processes, because the 'security' in question is everybody's security. If it is the nation's, and everybody's security, then these processes have to be more democratic. He pointed out that the organic movement building around the Save the Internet campaign illustrated well the strengths of the multistakeholder participatory model of policy making.

Anja added that the success of the Save The Internet movement was possible only because TRAI had an open and comprehensive consultation process. She concluded that addressing the need for more such spaces is, therefore, of utmost importance.
Indeed, if there was one overarching takeaway from the meeting, it was perhaps this: whether to discuss cybersecurity or other Internet governance issues, it is the development of a strong system of multistakekholder engagement in India that is the need of the hour in this field.

List of participants

1. Rekha Jain - IIM Ahemdabad
2. Kannamma Raman - University of Mumbai
3. Gayatri Khandhadai- APC
4. Anivar Aravind - Indic Project
5. Rachita Taneja - Jhatkaa.org
6. Amrita Choudhary - CCAOI
7. Kamala Sripada - CNN-IBN
8. Vinay Kesari - Lawyer
9. Rahul Sharma -DSCI
10. Nehmat Kaur - SFLC
11. Arjun Jayakumar - SFLC
12. Shalini S - CCG NLUD
13. Aditya Bhatia - DSCI
14. Jyoti Pandey - CIS
15. Kiran Jonnalagadda - Internet Freedom Foundation
16. Apar Gupta - Lawyer
17. Samiran Gupta - ICANN
18. Rajat Kumar - DEF
19. Neha Alawadhi - Economic Times
20. Arul R - IDSA
21. Aditya Dipankar - FOLO
22. Kim Arora - Times of India
23. Sajan Kuriakos - CHRI
24. Amber Sinha - CIS
25. Anja Kovacs, Internet Democracy Project
26. Rajat Rai Handa, Internet Democracy Project
27. Nayantara Ranganathan, Internet Democracy Project
28. Saikat Datta, Internet Democracy Project