CIS Submission to UN High-Level Panel on Digital Cooperation

January 2019

Authors (in alphabetical order): **Aayush Rathi**, **Ambika Tandon**, **Arindrajit Basu** and **Elonnai Hickok**

The Centre for Internet and Society (CIS), India
https://cis-india.org

Authors (in alphabetical order):
Aayush Rathi, Ambika Tandon, Arindrajit Basu and Elonnai Hickok
Organisation: Centre for Internet and Society, India
Stakeholder Group: Civil Society
E-mail: arindrajit@cis-india.org, aayush@cis-india.org

Guiding Questions

1) Values and Principles:
a) What are the key values that individuals, organizations, and countries should support, protect, foster, or prioritize when working together to address digital issues?

While there are a large number of values that individuals should look to address when working together to enhance the use of the digital sphere for everyone, over the course of our research we felt that four key values stood out:

1. Development oriented ICTs
A development dimension of cyber cooperation should be built on four fundamental tenets: (a) Information infrastructure as an utility and entitlement for every citizen in terms of accessing services, (b) Empowerment of citizens through social and financial inclusion, and (c) Enabling access to information infrastructure through education, awareness and capacity to use digital resources. In order to enable all nations to harness digital infrastructure for the furthering of socio-economic and security objectives, states then need adequate resources including skilling and financial resources for (d) using ICTs for furthering socio-economic rights and civil and political rights in line with both the United Nations Sustainable Development Goals 2030 and commitments made by various countries to the International Covenant on Civil and Political RIghts (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR) [1].

Thus far, global discourse on norms for cyber stability has been limited to the First Committee of the United Nations General Assembly, which limits itself to Disarmament and International Security Affairs [28]. It should be looked as a crucial tool towards meeting the United Nations Sustainable Development Goals in 2030 [2]. As of now, the ‘Big Data for Development’ discourse at the UN is progressing independently of norms for responsible state behaviour in cyberspace. A merging of these two strands by promoting a norm underscoring international co-operation on utilising ICTs for sustainable development might be useful for the Global South.

2. Human centric development of ICTs
Cooperation in the digital realm should be human centric and promote human interaction and cooperation through the use of technology rather than replace human interaction with technocratic tools of governance. One of the conclusions of our research on the use of Artificial Intelligence was that we need to devise a regulatory spectrum around the use

of Artificial Intelligence which will conceptualise the extent of regulation based on the three following human-centric factors [3]:

- Modeling Human Behaviour: An AI solution trying to model human behaviour, as in the case of judicial decision-making or predictive policing may need to be more regulated, adhere to stricter standards, and need more oversight than an algorithm that is trying to predict 'natural' phenomenon such as traffic congestion or weather patterns.
- Human Impact: An AI solution which could cause greater harm if applied erroneously-such as a robot soldier that mistakenly targets a civilian requires a different level and framework of regulation than an AI solution designed to create a learning path for a student in the education sector and errs in making an appropriate assessment.
- Primary User: AI solutions whose primary users are state agents attempting to discharge duties in the public interest such as policemen, should be approached with more caution than those used by individuals such as farmers getting weather alerts.

3. Security and Privacy in the development and use of ICTs

Security and privacy should underpin and be built into online cooperation and infrastructure meant to facilitate the same. We believe that these two principles are related and the trade-off is often a false one. Therefore, our cyber security project looks at the concept of security as a bottom-up phenomenon where the focus is on the individual feeling secure through an assessment of subjective parameters as opposed to a technocratic decision made by the state on what may constitute objective standards for cyber security. For this reason, we consider data protection and privacy as a core part of our cyber security research agenda.

4. Grounding in international human rights norms and thresholds of legality

All uses of ICTs and policies regulating the digital sphere should be grounded in universally acknowledged principles of international human rights norms and accepted thresholds of legality. While we acknowledge that the applicability of various bodies of international law to cyberspace continues to be disputed, we believe that reference to international law as a set of values for facilitating positive conflict and continued dialogue among stakeholders holds a lot of promise.

b) What principles should guide stakeholders as they cooperate with each other to address issues brought about by digital technology?

- **Open and transparent channels of communication, oversight and grievance redressal:** The digital realm can enable cooperation across sectors, stakeholder groups, and contexts. From our experience as a research organization, openness and transparency in our actions and thought process can work to enable trust and catalyze collaboration. We have also observed that often grievance redressal mechanisms are unknown or inaccessible to various stakeholders and opening up channels of communication to facilitate avenues of the same both in conjunction with the state and private actors who play a key role in this space is vital going forward.

- **Inclusiveness:** Cooperation in the digital realm benefits from inclusion of all voices and perspectives despite differences in positions or ideology. Often, the agenda for driving cooperation is set by thinkers from select geographic parts of the world because they have the economic and intellectual capacity to drive this discourse. We encourage increased participation from research and academia from all parts of the world, which is naturally contingent on adequate funding and an enabling environment for quality research.
- **Evidence based:** Cooperation in the digital realm should be based on evidence and should seek to facilitate knowledge creation and exchange. This necessitates field work and extensive consultations with stakeholders, particularly at the grassroots level. In this context, research organisations approaching digital co-operation from a variety of angles should look to work both with grassroots processes, citizen-driven movements and the government to lend nuance to discourse. Often, research on digital issues is not communicated to all individuals due to the asymmetries in technological or legal comprehension. Therefore, funding of research projects should be pooled into diverse contexts and spread among a variety of stakeholders with an eye on actual and potential impact of each grant.
- **Constructive Criticism:** While it is important to critically examine an issue, constructive criticism oriented towards solutions allows for conceptualising the next steps. Civil society actors, security researchers and private corporations should look to work with the government to aid in the development of inclusive and efficient institutions.
- **Differentiation of responsibilities based on due diligence**: It is clear that all states and stakeholders cannot equally contribute to cyber stability or to fair cooperation in cyberspace. However, it is expected that all states should attempt to contribute within the constraints of their resources and capacity.

The ILC Draft Articles on Liability for Transboundary Harm have laid down a due diligence obligation [4]. The Commentary articulates that a due diligence obligation requires reasonable efforts by a State to inform itself of factual and legal components that relate foreseeably to a contemplated procedure and to take appropriate measures in a timely fashion to address them [5].

The International Court of Justice has stated that due diligence is an obligation of conduct and not of result [6]. The due diligence standard should be evaluated on a two-pronged test - of knowledge and capacity [7]. The knowledge prong entails assessment of whether the state possessed the knowledge of a specific cyber attack or whether it ought to have known about the operation given the means at its disposal ('Constructive Knowledge') [8]. The capacity prong entails that the state make full use of its institutional, resource and territorial capacity to detect cyber threats and prosecute them, if need be [9].

The due diligence principle has also been flagged off by Tallinn Manual 2.0 (Rule 7) which "requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of and produce serious adverse consequences for other states. [10]" The commentary does not lay down any guidelines on the duty of host states to prevent potential attacks, the duties of states through which the attack is routed and how the 'constructive knowledge' test applies to cyber operations [11]. At the same time, the Manual is clear that there is no duty to monitor cyber activities originating from their territory owing to surveillance concerns [12]. The lack of clear guidelines applying this obligation to cyberspace render it difficult for host states and the rest of the international community to determine whether due diligence obligations in cyberspace are being fulfilled {13].

c) How can these values and principles be better embedded into existing private and/or public activities in the digital realm?

We will use this section to address some of the mechanisms that should underpin the global processes attempting to formulate norms fermenting global cooperation in cyberspace and furthering digital stability. Many of these values were uncovered through research the commissioned by the Global Commission on Stability of Cyberspace that the Centre for Internet and Society has previously undertaken. [27]

1. Learning from history:

Policy-makers, including those working towards fostering cyber stability often use past analogous situations to frame questions and resolve pressing current issues.However, the potential lessons from history are limited if we are unable to understand the processes that built up to these situations and how they apply today [14]. To truly derive value from rich historical lessons, we embarked on an investigation that traced negotiation processes which lead to the forging of successful analogous universal regimes for global security and the the nature of normative contestation that enabled the evolution of the core norms that shaped these regimes. From this study, we derived some useful lessons that could underpin the development of a regime that sets uniform standards for the crafting of stability in cyberspace.

2. Promote ideas-in particular those coming from the 'forgotten'

As evident from our case studies, often the dawn of an all-encompassing regime are from ideas that emerge through conversations, correspondences and paper presentations by individuals, organizations or coalitions. The outlawing of war, which was essentially the brainchild of one commercial lawyer in Chicago or the emergence of the concept of the 'common heritage of mankind' which owed its birth to the speech of a nearly unknown Maltese delegate-Arvind Pardo. both originated as academic ideas that were then taken forward at the institutional level. Apart from academics, neutral non-governmental organisations can also play a crucial role. The ICRC's pre-draft of the Geneva Conventions and the Additional Protocols helped speed up the negotiations and served as the language of International Law that facilitated conflict initially and then finally, consensus.

3. Internal and External Transparency

There must be transparency in the bargaining process at two levels:

(1) Internal Transparency: This would be internal to the Parties and not necessarily the public Transparent strategic groupings may be the way forward in the short-run until universal minimum core markers of consensus may be found. Existing governmental groups and forums could be potentially leveraged such as the Freedom Online Coalition, the G7, or the G20 as spaces for consensus building on specific topic areas.
(2)Transparency of process and outcomes: This would be communicated to the public at large which would foster confidence in the negotiation process and thereby enable states to represent a wide array of domestic and international stakeholders in the proceedings.

4. Promoting Smart coalitions

Coalitions of like-minded states and stakeholders grouped by common ideology, interests, focus areas or identities may aid in fostering positive conflict, identifying key areas for consensus and in the development of a formula for co-operation in the long run. Given the intersectionality of identities and therefore, a convergence of the potential sources of discrimination, multiple coalitions that enable multiple actors to have their voice heard is encouraged.

As opposed to a fragmented approach to cyber governance,coalitions are an useful tool as it would allow for some certainty in the formation of strategic alliances and in national approaches to cyberspace. Coalition-building was successfully used to articulate varied state interests and anchor the negotiations throughout the UNCLOS process through groups such as the G77. We believe that creating 'smart coalitions' driven by co-operation on selective issues might set the ground for co-operation on a broader normative framework.

5. Wide participation from non-state actors

Wide participation by non-state actors can be key in negotiation processes. Identification of norm-entrepreneurs and supporting them may be important for a successful outcome.

Involvement of non-state actors can create external pressure for outcomes to be reached that are acceptable to the public, can contribute to the objectives of the agreement, and can play an important role in accountability at the national level of state commitments. At the same time, states are often reluctant to take initiatives on matters which would require an agreement at large as the transaction costs of facilitating consensus would be greater than the individual benefits of a stable regime. This however should not prevent a normative framework from emerging organically. Therefore, multi-stakeholder non-state bodies and forums pursuing multi-stakeholder models of Internet Governance such as the, GCSC, IGF, ICANN, ISO, ITU, and ISOC should continue to play a role-both in finding areas for collaboration, generating ideas, normative content, and developing standards that could inform a future agreement. These forums and bodies can also serve as spaces for bringing multiple actors to the table to discuss key issues and in doing so establish a foundation for future discussion. Such interactions are already taking place. Apart from non-governmental organizations, large private sector organizations most significantly affected by the weaponisation of cyberspace should also be consulted so that the formula agreed upon takes into account their experience, understanding, and requirements. It is crucial that governments also continue to engage with these non-state actors throughout the negotiation process. Microsoft's endeavours in promoting the Paris Call for Trust and Security in Cyberspace mark a positive step in the right direction but the success of the initiative is contingent on the range of actors they can rope in [29].

2) Methods and Mechanisms: a) How do the stakeholders you are familiar with currently address their social, economic, and legal issues related to digital technologies? How effective or successful are these methods/mechanisms for digital cooperation? What are their gaps, weaknesses, or constraints? How can these be addressed?

The economic restructuring underway in the digital space is bringing with it a complete reimagination of globalised labour chains, impacting labour conditions across the global North and South. Aspects of Industry 4.0, such as the impact of reshoring on employment in countries with economies dependent on providing low cost labour, are specific to Southern economies and need context-specific solutions. However, in our engagement with the future of work, we found that emerging agendas that aim to mitigate the impact of technological disruption continue to be driven by actors in the global North, underrepresenting concerns around reshoring or informality that are specific to the South [19]. One of the mechanisms to fill this gap would be to encourage South-South cooperation - limited not only to nation states, but also to networks of formal and informal workers. These transnational networks can support co-operation at the global level and co-ordination mechanisms like the UN should encourage multiple coalitions of this nature as well to facilitate information exchange [26].

In this respect, digital technologies have the potential to facilitate the formation of networks for mobilisation around issues such as collective bargaining, labour conditions, and minimum wages. As our work on the use of mobile phones by sex workers and sexual minorities demonstrated, these technologies have been used successfully by sex work unions and individuals to maintain networks to enhance safety, as well as mobilise around political issues. This is especially the case with social groups that face barriers to using other public spaces, such as persons with disabilities or non-binary individuals. However, using even basic mobile phones has translated into a higher level of harassment and violence for both sex workers and sexual minorities, as has been documented in the context of other marginalised communities [20].

These have been combated using structural mechanisms through intermediaries and law enforcement. Several flaws have been pointed out in each, some of which could lead to increasing censorship and constraints on freedom of expression that end up hurting minority groups rather than those in power. This includes regulations around hate speech, or banning of pornography by intermediaries and law enforcement to protect modesty of females. Violence against marginalised groups then need to be dealt with (a) making legal-institutional and technical solutions more accessible and responsive, and (b) developing community-based non-legal solutions to violence online. Often, the community based solutions are non-technological but are customary practices that hold more relevance in each context and work more effectively than top-down impositions of models configured and implemented in grossly different contexts. For example, Remi Rajeswari, who is a Police Officer in Telangana's Warnaparthy district has used folk singers and drummers to stifle the spread of fake news and disinformation on online platforms [15].

b) Who are the forgotten stakeholders in these mechanisms? How can we strengthen the voices of women, young people, small enterprises, small island states and others who are often missing?

The tendency to bundle together marginalised groups poses a threat to ongoing efforts aimed at their inclusion by foreclosing the specificity in approaches undertaken to enable greater societal inclusion. Within each marginalised group, homogeneity should not be assumed - the challenges posed by the digital divide need to be contextualised to, and based on, the intersectionalities of race, gender, class, caste (uniquely in India), sexuality and location. Doing so will allow the identification of unique challenges faced by such groups in an increasingly digitised and datafied environment - and should be the starting point in developing solutions that can address the specific challenges posed in this environment.

For instance, growing evidence indicates that a market-driven focus on connectivity has not led to a concomitant rise in women accessing the Internet; in fact, the gender divide in a lot of middle-income countries is increasing [16]. This implies that older concerns around affordability and access continue to remain relevant across most of the global South. For example, gender gaps in internet and mobile use are found be to higher in some richer Asian countries with high income inequality than some poorer African countries with lower disparity in income [17].

However, focusing on ‘access’ should not preclude accounting for digital capacities, which are also divided along gendered lines [18]. This is codified in the articulation of ‘ICTs for women’s rights’ in the Sustainable Development Goals (SDGs) review processes wherein access to ICTs is measured through the proportion of individuals who own a mobile telephone, by sex (SDG indicator 5. B.1.). This techno-deterministic articulation resists the need to account for the divide in digital capacities. The questions need to be further interrogated are along the lines of ‘access to what?’ and ‘access of what kind?’. The capability approach will allow for targeted policy-making approaches that will differently apply to different marginalities - from SMEs to children to women [21].

Digital capacities also need to be assessed in consonance with other capacities, such as literacy and education, which have consistently shaped the ability to access digital technologies or accrue benefits of participating in the digital economy. In fact, education and income have been found to be the primary determinants of the gender gap in access in use [17]. It is also crucial to note that the next set of people coming online in emerging economies have a heterogenous set of digital consumption and usage patterns that may be entirely distinct from the homogenous western, urban-centric patterns that have been studied and taken as the norm thus far. These new sets of consumption patterns offer a new set of vulnerabilities but also immense potential for the development of a truly global internet that has participation from a variety of groups-with an unique set of values and principles underpinning each individual’s engagement with the digital space.

Keeping this in mind, Centre for Internet & Society, along with Mission Publiques hosted a collaborative event on Citizens Day - a day where groups of hundreds of ordinary citizens met gathered information, discussed and delivered a collective view on the core stakes of digitalization. We used the participation of multiple individuals in the Internet ecosystem to help us represent India's views in this global debate. The participants were selected at random to represent their area of the world, and represented all stratas of society and a diverse set of identities.

c) What new or innovative methods/mechanisms might be devised for multi-stakeholder cooperation in the digital realm?

NATIONAL AND SUB-NATIONAL LEVEL:

At the national and sub-national level, engagement with the 'forgotten' voices in the digital arena can be facilitated with the integration of grassroots/on-ground organisations representing the voice of marginalised actors. This will enable the reimagining of legal and institutional mechanisms that need to be developed to mitigate the deleterious impact the digital economy may portend for gains that may have been made for the protection of rights of the marginalised. These mechanisms will have to be situated in the specific socio-economic and cultural realities of each geography as the digital economy will impact nations differently. For instance, low and middle-income countries are projected to be a greater risk of being impacted adversely in the future of work owing to a greater share of routine jobs that are susceptible to automation [22]. Further, in the short-term, such an approach could facilitate devising specific tools aimed at furthering self-help groups for those on the margins, such as cooperatives and local platform enterprises. In addition to supporting governments, private sector and other policy-drivers in fermenting nuanced and inclusive discourse,research organisations could play a crucial role in supporting a variety movements by providing a strong foundational body of knowledge enable the accomplishment of goals being strived for. In the space of conducting research, a participatory approach geared towards achieving political goals is a useful methodological approach to undertake. This could be achieved by involving some of the members of the community being researched as the researchers. Employing principles of feminist methodology [23], such an approach could serve the dual purpose of both building solidarity networks while also encouraging the development of local knowledges useful in sustaining projects beyond the practical encumbrance of funding and time considerations that accompany research projects.

Having said that, this approach needs to be met with top-down attempts at arriving at engaging in norms development around decent work in the 'networked information economy' [24]. These will have to account for the clout that transnational corporations in the digital economy enjoy [25] and would extend to holding them accountable for the protection of human rights. This needs to be supplemented by the evolution of stronger rights-based data governance frameworks that go beyond individualistic notions of privacy and data protection. Such conceptions can be arrived at by incorporating feminist perspectives that allow for initiating a move away from a depoliticised neoliberal idea of techno-determinism, and towards community-centred and participatory governance technological implementations.

The Centre for Internet and Society began privacy research in 2010. Amongst other objectives, our research sought to enhance the discourse around privacy in India and bring more and needed stakeholders into the debate. To do this we held roundtables across the country in collaboration with law schools, consumer groups, and industry bodies. We undertook case studies to document gaps between policy and implementation of the same. To ensure the voices of citizens were heard and documented, we held roundtables tables to discuss and document comments on a 'citizens privacy bill we had drafted.

INTERNATIONAL LEVEL:
Any global process facilitating cyber co-operation must be cognizant of the five following parameters that had proved useful when planning the NetMundial Initiative:

1. **Stakeholders:** It demarcated the categories of participants in the discussion into (largely) five: governments, civil society, private sector, academia, and the technical community. Representatives from each stakeholder group should be allocated equal time. Further, as indicated above, it must be recognized that all stakeholder groups are not homogenous and in order to prevent each group from getting cartelised, due regard must be shown to the time allotted to each intersectionality.

2. **Secretariat:** The Secretariat of global bodies must be representative of various interest groups,nationalities and identities. As the body responsible

3. **Remote participation:** Remote participation must be implemented in a manner that encourages and facilitates inputs from external stakeholders unable to physically participate in meetings via video-conferencing.

4. **Pre meeting consultations/Inter-sessional work**: All global processes should be underpinned by extensive inter-sessional work through online consultations and off-site meetings that enables inclusive participation.

5. **Transparency:** Transparency in the functioning of all global processes must be ensured through its operations procedures. All minute of discussions, exchanges and communication at the conference must be made public for comment by external stakeholders.

3) Illustrative Action Areas: The Panel plans to explore the following areas, among others, where greater digital cooperation is required: • inclusive development and closing the digital gap • inclusive participation in the digital economy • data • protection of human rights online, particularly of children, women and marginalized communities • human voice and participation in shaping technological choices and architecture • digital trust and security • building the capacity of individuals, institutions and governments for the digital transformation. a) What are the challenges faced by stakeholders (e.g. individuals, governments, the private sector, civil society, international organizations, technical and academic communities) working together in these areas? b) What are successful examples of cooperation among stakeholders in these areas? Where is further cooperation needed? c) What form might cooperation among stakeholders in these areas take? What values and principles should underpin it?

We hope that we have addressed these questions through our responses in Section II that dealt with some of the concrete areas identified by the Panel. These are all important action areas and we are confident that the Panel will approach each of them with a context-specific, human-centric and constructively oriented approach that is supported by the nuances of research at every level. We hope that, as the panel continues its work, further consultation will be requested on more specific topics than the high-level issues addressed here. This would serve as a platform for exchange among stakeholders who may not be geographically connected but are caught up in the entangled nature of cyberspace.

Endnotes

[1] Mukerji, Amb. Asoke (2018). India’s strategic interests in the norms formulation process.(Presentation made at The Centre for Internet and Society Symposium on India’s Cyber Strategy, 31 Aug 2018, New Delhi

[2] Un.org. (2019). Big Data for Sustainable Development. [online] Available at: http://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html [Accessed 1 Feb. 2019].

[3] Sinha, A., Hickok, E. and Basu, A. (2018). AI in India: A Policy Agenda. The Centre for Internet and Society. Available at: https://cis-india.org/internet-governance/blog/ai-in-india-a-policy-agenda

[4] International Law Commission. (2001). Commentary to Draft Articles on Prevention of Transboundary Harm. pp.71.

[5] International Law Commission. (2001). Commentary to Draft Articles on Prevention of Transboundary Harm. pp.71.

[6] Lammers, J. (1984). Pollution of International Water Courses: A Search for Substantive Rules and Principles. BRILL, pp.524.

[7] Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb & Mont.) [2007] ICJ 2 (Feb. 26) ¶ 430.

[8] Henderson, C. (2013). Trapp, State Responsibility for International Terrorism: Problems and Prospects, Oxford, Oxford University Press, 2011, 295pp., ISBN 9780199592999 (h/b). Leiden Journal of International Law, 26(01), pp.229-234.

[9] Henderson, C. (2013). Trapp, State Responsibility for International Terrorism: Problems and Prospects, Oxford, Oxford University Press, 2011.

[10] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press.

[11] 1) Clearly defined cyber security policy and/or legislation, 2) Use of government funds to create nodal agencies responsible for cybersecurity, 3) Continuous communication if any hazardous cyber activities are detected, 4) Response to any requests for evidence by international bodies

[12] Efrony, D. and Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), pp.583-657.

[13] Efrony, D. and Shany, Y. (2018). A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice. American Journal of International Law, 112(4), pp.583-657

[14] Richard E Neustadt and Ernest R May, Thinking in Time : The Uses of History for Decision-Makers, 1st FreePress pbk. ed. 1988 (New York : Free Press, 1988), accessed 6th May 2018, https://trove.nla.gov.au/version/44808522.

[15] Think Change India. (2018). Song by song, this woman IPS officer is helping quash fake news. Available at: https://yourstory.com/2018/07/song-by-song-this-woman-ips-officer-is-helping-quash-fake-news/

[16] Alliance for Affordable Internet - A4AI (2016). Digging into Data on the Gender Digital Divide. Available at: https://a4ai.org/digging-into-data-on-the-gender-digital-divide/

[17] Ageuro, A., Galpaya, H. and Gillwald, A. (2018). After Access: Understanding the Gender Gap in the Global South. Available at: http://afteraccess.net/wp-content/uploads/2018-After-Access-Understanding-the-gender-gap-in-the-Global-South.pdf

[18] Gurumurthy, A and Chami, N. (2017). What has the future of digital economy and society got to do with women's rights?. IT for Change. Available at: http://itforchange.net/sites/default/files/add/What%20has%20the%20future%20of%20digital%20economy%20and%20society%20got%20to%20do%20with%20women%27s%20rights%3F.pdf

[19] Rathi, A., Hickock, E. and Bidare, P. (Forthcoming). Future of Work in the IT/IT-eS Sector. The Centre for Internet and Society.

[20] Gurumurthy, A. and Vasudevan, A. (2008). Masculinity, Femininity, Equality – Gender Scripts in the Lives of the Born Digital, IT for Change. Available at: https://itforchange.net/masculinity-femininity-equality

[21] Kleine, D. (2010). ICT4WHAT? - Using the choice framework to operationalise the capability approach to development. J. Int. Dev., 22, pp.674-692.

[22] World Trade Organisation (2017). Impact of technology on labour market outcomes. Available at: https://www.wto.org/english/res_e/booksp_e/wtr17-3_e.pdf

[23] Tandon, A. (2018). Feminist Methodology in Technology Research: A Literature Review Centre for Internet and Society. Available at: https://cis-india.org/internet-governance/blog/ambika-tandon-december-23-2018-feminist-methodology-in-technology-research

[24] Benkler, Y. (2006). Wealth of Networks. Yale University Press.

[25] Gray, A. (2017). These are the world's 10 biggest corporate giants. World Economic Forum. Available at: https://www.weforum.org/agenda/2017/01/worlds-biggest-corporate-giants/

[26] Keck, M. and Sikkink, K. (1999). Transnational advocacy networks in international and regional politics. International Social Science Journal, 51(159), pp.89-101.

[27] Hickok, E. and Basu, A. (2018). Conceptualizing an International Security Architecture for Cyberspace. Available at: https://cis-india.org/internet-governance/files/gcsc-research-advisory-group.pdf

[28] Basu, A. and Hickok, E. (2018). Cyberspace and External Affairs: A Memorandum for India. Available at: :https://cis-india.org/internet-governance/blog/arindrajit-basu-and-elonnai-hickok-november-30-2018-cyberspace-and-external-affairs

[29] Basu, A. (2018). Private-Public Partnership for cybersecurity, Available at: https://www.thehindubusinessline.com/opinion/private-public-partnership-for-cyber-security/article25821899.ece