THE CENTRE FOR internet & society

Cyberspace and External Affairs: A Memorandum for India

Authors: Arindrajit Basu & Elonnai Hickok

Editors: Aayush Rathi & Shruti Trikanad

https://cis-india.org/

ACKNOWLEDGEMENTS

The insights in this brief benefited greatly from the discussion at the symposium on India's cyber strategy organised by the Centre for Internet&Society in New Delhi on August 31,2018. The speakers at this conference were Amb. Asoke Mukerji, Mr.Parminder Jeet Singh and Ms.Madhulika Srikumar. All errors and inaccuracies, however remain our own.

Executive Summary

This memorandum seeks to summarise the state of the global debate on the framing of norms for the regulation of cyberspace; outline how India can craft it's global strategic vision and finally, provides a set of recommendations for the MEA as they craft their cyber diplomacy strategy. It limits itself to advocating certain procedural steps that the Ministry of External Affairs should take towards propelling India forward as a leading voice in the global cyber norms space and explains why occupying this leadership position should be a vital foreign policy priority. It does not delve into content-based recommendations at this stage.

Further, this memorandum is not meant to serve as exhaustive academic research on the subject but builds on previous research by CIS in this area to highlight key policy windows that can be driven by India. [1]

This memorandum provides a background to global norms formation focussing on key global developments over the past month; traces the opportunities s for India to play a lead role in the global norms formulation debate and then charts out process related recommendations on next steps towards India taking this forward.

[1] For a more exhaustive treatment of various legal and political questions in the norms formulation debate and India's approach to this regime, please consult our paper titled '*The Potential for the Normative Regulation of Cyberspace: Implications for India.*' For a more exhaustive treatment of efforts towards norms formulation in other regimes consult our paper entitled *Conceptualizing an International Security architecture for cyberspace.*

Introduction

Information Communication Technologies (ICTs) have become woven into every aspect of life in the twenty-first century. Individuals, government institutions and the private sector increasingly rely on cyberspace for discharging economic, social and political functions. Yet, this increased usage and inter-dependence has come with a gamut of vulnerabilities and threat vectors, which can only be addressed through collaboration between states, private actors and civil society at the global level. While the global debate on cyber norms formulation has existed since the turn of the century, global co-operation in cyber norms formation has seen its peaks - with a consensus document emerging out of the 2015 report of the United Nations-Group of Governmental Experts (UN-GGE)[2], and troughs - such as the failure of the 2017 GGE to arrive at a consensus report.[3]

States have recognised the need to craft norms that can regulate the use of cyberspace and preserve its security and stability for years to come. However, this normative push to precipitate shared notions of cyber governance has yet to bear fruition for three key reasons.

1. There is a global cultural divide on the nature of cyberspace itself. The first group of states - driven by the US and backed up by G7 and EU countries perceives the internet as a free-flowing entity that should be driven largely by market competition globally and some government regulation, while also being observed and advised by civil society, in a process known as multi-stakeholderism. The second group - Russia, Iran and China prioritize state control over national cyber borders in a bid to preserve 'information sovereignty.' In many ways, the cyber norms divide is structured along Cold War lines, where the neoliberal democratic ideology is confronted by information control and authoritarianism. India has not yet committed itself firmly to any group and has the flexibility to craft a strategy that is allied with its interests.
2. The difficulties of tracing back and attributing a cyber attack to the original perpetrator incentivises states and non-state actors to continue engaging in

[2] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, paras. 9–15,UN Doc. A/70/174 (July 22, 2015) [hereinafter 2015 GGE Report]

[3] Michael Schmitt and Liis Vihul, "International Law Politicized: The UN GGE's failiure to advance cyber norms," Just Security, Jun 30 2017, accessed Nov 18,2017, at [hereinafter 'Schmitt Just Security']

low-level cyber attacks against states who retain military and strategic advantages in the traditional domains of warfare. This is because the attacker may perceive the benefits of mounting a cyber-attack as outweighing the risks of getting caught

3. There has been an increasing participation of heterogeneous non-state actors in the global cyber-security architecture - both as perpetrators of cyber attacks and norm-entrepreneurs. This heterogeneity in needs, motivations and ideologies of these actors poses an obstacle to developing a uniform and cohesive approach to cyber regulation.

While there was a relative lull in the norms formation process in 2017, this process is now back in full swing with two resolutions, sponsored by the US and Russia respectively, being passed by the United Nations General Assembly/ (UNGA). India voted for both these resolutions presented at the UNGA First Committee on Disarmament and International Security[4], which means that it now has the opportunity to opt for an approach it feels is strategically beneficial or devise a new approach, focusing on other aspects of norms formulation, which have been neglected in the debate thus far. **India should play a pro-active role in driving the norms-formulation agenda, rather than following an agenda driven and defined by other states.** As this brief will explain,as a key country in the region, Indian civil society, Indian research organisations, and Indian private sector companies are becoming an increasingly critical part of global norms formulation process. This, along with India's past engagement, creates a crucial opportunity for the government through the Ministry of External Affairs (MEA) to engage in a meaningful way and contribute distinct and unique interventions to influence and shape the cyber norms debate and process.

[4] http://webtv.un.org/search/first-committee-31st-meeting-general-assembly-73rd-session/5859584578001/?term=First%20Committee

Background to Global Norms Formation

The possibility of a cyber- attack caused Russia in 1998 to propose a treaty at the United Nations that would regulate and restrict the utilization of cyber-attacks and cyber weapons.[5] The USA rejected this proposal and it went on to find little support.[6]Further research on non-binding norms and confidence building measures as alternatives to the development of a full-fledged treaty regime lead to the international community pivoting towards this approach.[7] They attempted to follow the norms-driven approach set up through regimes such as the Missile Technology Control Regime (MTCR). This resulted in the birth of the UN-GGE process. The GGE was set up in 2004 and comprised independent experts from 15 states. This group was designed to advise the UN on promoting peace and stability in cyberspace. [8] The 2015 report of the fourth UN-GGE elaborated on these concepts and laid down a comprehensive framework for further discussion on cyber norm evolution. Section III of the report lays down several norms, rules and principles for responsible state behaviour in cyberspace. [9]

These include:

• Not knowingly allowing their territory to be used for the commission of internationally wrongful acts using Information Communication Technologies (ICTs);

[5] James Andrew Lewis, “ Revitalizing Progress on International Negotiations in Cybersecurity” in Osler Hampson and Michael Sulmeyer, Getting Beyond Norms:New approaches to cybersecurity challenges (Centre for Governance and Innovation, 2017), 13

[6] Ibid

[7] Ibid

[8] Eneken Tikk and Mika Kerttunen, The Alleged Demise of the UN-GGE: An autopsy and eulogy (Cyber Policy Institute,2017), at 17, at , accessed January 6 2018. [hereinafter ‘Tikk and Kerttunen’] [Even though the first UN-GGE was unable to agree upon a report, the second GGE was able to garner more consensus and released a report in 2010. The third GGE presented its report in 2013 and agreed on a set of founding norms for the governance of cyberspace.

The document expressed that international law, state sovereignty and human rights were applicable to the governance of cyberspace. Further, the report also stated that states must not use non-state proxies to commit cyber- attacks on other states or allow non-state actors to use their territory for the launching of cyber-attacks.

[9] These include

• Not knowingly allowing their territory to be used for the commission of internationally wrongful acts using Information Communication Technologies (ICTs);

• To cooperate for the exchange of information using ICTs

• Refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations

•To not knowingly supporting ICT activity contrary to the principles of international law.

• To cooperate for the exchange of information using ICTs
• Refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations
•To not knowingly supporting ICT activity contrary to the principles of international law.

Drawing from what appeared to be universal consensus on the norms process a fifth GGE was instituted by the United Nations "to study, with a view to promoting common understandings,...how international law applies to the use of information and communications technologies by States, as well as norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building...." [10] However, due to what cyber security and International Law expert and chair of the Tallinn Manual Process, Prof. Michael Schmitt terms the 'politicization of cyber norms,' the 2017 UN-GGE was not able to arrive at consensus due to stonewalling by Cuba and reportedly China and Russia.

Gauging from Cuba's publicly available statement, the UN-GGE disagreed on three fundamental questions. It appears from their statement that they believe that applying the traditional rules of international law to the cybersphere would convert it into a 'theatre of military action' and legitimize unilateral punitive sanction. Mike Schmitt criticizes this position - claiming that it has no validity in international law and is being utilised by states to gain an asymmetric strategic advantage. The states engaging in the stonewalling are rarely the victims of unlawful cyber attacks. [11]

Further, as stated by Arun Mohan Sukumar, the dissenting states did not want the rules of the game to be dictated by militarily advanced states.[12] Sukumar goes on to criticise this approach, even in terms of its strategic validity as predictability in cyberspace is an end that all states should desire[13]

De-legitimizing the progress made by the 2016-17 GGE through an excessive focus on International Law was thus possibly a flawed approach. The only two publicly available

[10] Michael Schmitt and Liis Vihul, "International Law Politicized: The UN GGE's failiure to advance cyber norms," Just Security, Jun 30 2017, accessed Nov 18,2017, at [hereinafter 'Schmitt Just Security'
[11] Ibid
[12] Arun Mohan Sukumar," The UN-GGE failed: Is International Law in cyberspace doomed?",Lawfare, July 4,2017, accessed Nov, 18, 2017, https://www.lawfareblog.com/ungge-failed-international-law-cyberspace-doomed-well
[13] Ibid

statements made by state representatives to the GGE are those of Cuba and the United States.

It appears therefore that the GGE broke down due to a lack of consensus on
1. Response to internationally wrongful acts (countermeasures in cyberspace),
2. Self-Defence in cyberspace, and
3. The applicability of International Humanitarian Law to cyberspace.

There are two crucial fissures in the norms formation process across two groups of states. The first one revolves around the question of sovereignty. The Sino-Russian view suggests that sovereignty in international law is absolute and no entity other than the sovereign state itself can limit the exercise of this power, which is directly at odds with the desire of the US and like-minded states to preserve the free-flow of information.

Recent developments in 2018

Despite the breakdown in 2017, multiple norms formulation processes have opened up over the past year and have made some concrete progress.. Though these processes are a positive in that they recognize the criticality of norms for cyber space, a potential concern is the fragmentation of the norms formulation process, which would allow for the more powerful state and non-state voices to have a greater say in the debate.[14] This is for two reasons. First, as these actors have greater financial capacity, they would be able to fund delegations attending a greater number of conferences/forums or organize/sponsor such events. Second, if they were numerically outnumbered in forums such as the UN, they could simply 'exit' these forums and promote their agenda in another one. Such fragmentation is something India should look to guard against and thus seek out forums which might consolidate norms formulation efforts.

The developments have occured at the following levels:

1. **Inter governmental:** United Nations
2. **Private sector:** Tech Accords, Digital Geneva Convention and Charter of Trust
3. **Multi-stakeholder (without formal representation from states):** Global Commission on Stability of Cyberspace

[14] Eyal Benveniisti and George Downs," The Empire's New Clothes: Political Economy and the Fragmentatin of International Law"60 STANFORD LAW REVIEW (2007),<https://www.stanfordlawreview.org/print/article/the-empires-new-clothes-political-economy-and-the-fragmentation-of-international-law/>

4. **Multi-stakeholder (intended to incorporate universal state representation):** The Paris Call for Trust and Security in Cyberspace

1. *United Nations* **(Inter-governmental)**

This fissure was reflected in the tabling of two competing resolutions at the First Committee of the United Nations General Assembly (UNGA) (on Disarmament and International Security) which concluded its 73rd session in New York on 8th November, 2018. [15] **(Compilation of votes in Annex 1)**

The resolution tabled by the Russian Federation entitled 'Developments in the field of information and telecommunications in the context of international security'[16] was passed by a vote of 109 in favour to 45 against, with 16 abstentions. The resolution encapsulated the Sino-Russian view.[17] Keeping in line with the divide at the GGE and the historical divide in cyberspace, most of the 45 votes against this resolution came from Western Europe and North America, accompanied by Japan, Australia and New Zealand-allies of the US in the Asia-Pacific region.

The UNGA also approved the draft resolution "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security" tabled by the United States, with 139 in favour to 11 against, with 18 abstentions.[18] Most of the eleven votes against came from South America and the Middle East, along with Russia and China.

India voted for both resolutions. This was a well thought out vote, which can be seen as a product of its recent pivot towards positive relations-with both Russia and USA.[19] The vote now enables India to respond to policy windows and build on positive aspects of both approaches to ferment an approach that caters to the needs of the region and the developing world.

The abstentions in both resolutions came from African states, who are possibly yet to formulate a clear policy on their approach to cyber norms, or are reliant on both USA and

[15] Grigsby, A. (2018)' Unpacking the competing Russian and U.S. cyberspace resolutions at the United Nations' <https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations>

[16] http://undocs.org/A/C.1/73/L.27

[17] https://www.un.org/press/en/2018/gadis3619.doc.htm

[18] https://www.un.org/press/en/2018/gadis3619.doc.htm

[19] Rajesh Basrur(2017) " Modi's Foreign Policy:A trajectory unchanged"https://www.chathamhouse.org/sites/default/files/publications/ia/INTA93_1_02_Basrur.pdf

western European countries on one hand and Russia and China on the other. It is crucial that their voices do not get drowned out of the debate due to geo-political reasons and power politics.

The UNGA also took cognizance of the future steps directed by each resolution. As prompted by the text of the Russian Resolution, the UNGA agreed to constitute an open-ended working group that would act on a consensus basis to further norms, rules and principles of responsible behaviour in cyberspace.[20] As per the text of the US resolution, the UNGA would request the Secretary-General, with the assistance of a group of governmental experts (GGE) to continue studying the norms formulation process and present their finding at the seventy-sixth UNGA in 2021.[21] It also calls for an Annex to the report that consolidates contributions from governmental experts on how International Law applies to the utilisation of ICTs by states.[22] **Both these initiatives offer an opportunity for India to make its voice and leadership role felt at the inter-state level.**

3. *Tech Accords, Digital Geneva Convention and Charter of Trust* **(Private Sector)**

The private sector has increasingly recognised the value of stability in cyberspace-partly because their revenue model depends on trust and security in digital communication and partly because they need to act as responsible global political actors in response to public expectation.[23] **While the MEA cannot directly engage with the private sector initiatives, it is crucial for the MEA to remain abreast of the commitments made by the private sector and also work towards ensuring that the private sector actors in India also have a say in framing these agreements, in order to make them more representative.**

Both the Tech Accord and the Digital Geneva Conventions are initiatives pioneered by Microsoft. The Tech Accord is “a public commitment among more than 30 global companies to protect and empower civilians online and to improve the security, stability,

[20] http://undocs.org/A/C.1/73/L.27, Clause 5
[21] https://undocs.org/A/C.1/73/L.37, Clause 3
[22] *Ibid*
[23] Hurel, Louise Marie and Lobato, Luisa, Unpacking Cybernorms: Private Companies as Norms Entrepreneurs (January 22, 2018). GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017. Available at SSRN: https://ssrn.com/abstract=3107237 or http://dx.doi.org/10.2139/ssrn.3107237

and resilience of cyberspace."[24] In April of 2018, 34 companies in the U.S. and Europe signed and published the Tech Accord, "agreeing to defend all customers everywhere from malicious attacks by cybercriminal enterprises and nation-states."[25] The list of signatory companies has now grown to 69.[26]

The four pillars of the Tech Accords are 1) Stronger Defense, 2) No Offense, 3) Capacity Building and 4) Collective Action.

The Digital Geneva Convention, on the other hand is a set of principles aimed at states with the objective of reducing collateral damage as a result of offensive cyber action. The principles include: 1) Restraint in the development of cyber weapons, 2)No targeting of tech companies,private sector or critical infrastructure, 3)Assist private sector efforts to detect, contain, respond to, and recover in the face of cyberattacks, 4)Agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities,5)Agree to limit proliferation of cyber weapons and 6)Limit engagement in cyber offensive operations.

Siemens has also put forward a Charter of Trust-which was signed by a number of European tech companies, such as Airbus, Daimler and Allianz and was released at the Munich Security Conference on May 17, 2018.[27] This tells us that Europe-based companies are also aware of the realities of increasing digitization.[28]

3. Global Commission on Stability of Cyberspace **(Multi-stakeholder without formal representation from states)**

Along with the UN-driven process, global multi-stakeholder initiatives are also attempting to guide states into advocating norms that may be beneficial for cyber stability.The Global Commission on the Stability of Cyberspace (GCSC) is a key player in this space. It is a multi-stakeholder initiative of the Hague Centre for Strategic Studies and the East

[24] https://cybertechaccord.org/
[25] *Ibid*
[26] https://cybertechaccord.org/global-expansion/
[27]https://www.siemens.com/innovation/en/home/pictures-of-the-future/digitalization-and-software/cybersecurity-charter-of-trust.html
[28]Available at https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/shi-13378-cot-dok-narrative-online-2018-02-13-sbi-en.pdf

West Institute that seeks to promote mutual awareness and understanding among various cyberspace communities. It works towards developing a coherent set of norms and policies that advance the stability and security of cyberspace.[29]

Chaired by Marina Kaljurand, and Co-Chaired by Michael Chertoff and Latha Reddy, the Commission has 26 Commissioners who are experts representing a wide range of geographic regions and multiple communities including academia industry, government, technical and civil society[30]. Dr. Samir Saran, President of the Observer Research Foundation (ORF) in New Delhi is a Commissioner at the GCSC.[31] Both ORF[32] and CIS[33] have contributed research to the Briefings of the Research and Advisory Group (RAG) of the GCSC.

On the 8th of November, the GCSC also announced the release of a norms package that proposed six new norms that were a product of extensive deliberations made by the Commission.[34] These norms focus on the following areas:

- Norm to Avoid Tampering[35]
- Norm Against Commandeering of ICT Devices into Botnets
- Norm for States to Create a Vulnerability Equities Process
- Norm to Reduce and Mitigate Significant Vulnerabilities
- Norm on Basic Cyber Hygiene as Foundational Defense
- Norm Against Offensive Cyber Operations by Non-State Actors

These norms are valuable guiding principles in taking the norms formulation process forward. **It would be useful for India to craft out a strategy that makes these norms work effectively given its socio-economic position and that of similarly positioned states.**

[29] https://cyberstability.org/about/
[30] Ibid
[31] https://cyberstability.org/commissioners/samir-saran/
[32] https://cyberstability.org/research/briefings-and-memos-of-the-research-advisory-group/
[33]https://cyberstability.org/news/gcsc-issue-brief-2-briefing-and-memos-from-the-research-advisory-group/
[34] https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf
[35] This had been published earlier in May 2018 <https://cyberstability.org/research/global-commission-urges-protecting-electoral-infrastructure/>

4. Paris Call for Cyber Security (**Multi-stakeholder with intended formal representation from states, private sector, academia and civil society**)

On 12th November, 2018, the Paris Call for Trust and Security was announced by President Emmanuel Macron at the UNESCO Internet Governance Forum (IGF). This document contains a set of commonly accepted high-level principles for global cyber stability, largely stemming from the consensus document that emerged out of the 2015 GGE.[36] It has been endorsed by over fifty states, two hundred private sector entities and over one hundred organisations from civil society and academia. [37]

This initiative is being driven by Microsoft in conjunction with the French government. Both Microsoft and the French government are cognizant of the problem of fragmentation, and the Paris Call is meant to be the beginning of a process that brings together existing strands of discussion between government, industry, and civil society. The signatories to the Cybersecurity Tech Accord and the Siemens Charter of Trust have collectively endorsed the Paris Call.

[36] https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[37] https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pd

Reasons for India to Lead Global Cyber Norm Formation

India should build on and expand existing contribution to international cyber norms formation processes towards taking on a leadership role regionally and globally for three reasons:

Strategic interests

With the global cyber norms formulation in a state of flux at the institutional level, **India has an unique opportunity to pick up the pieces from the negotiations and emerge as a key player in the international arena by setting out its vision for the 'rules of the road' in cyberspace and garnering support for the same**. Such a vision needs to tie into and be supported by a strong and harmonized national cyber security roadmap.

India has played this role-as a crucial advocate for the interests of the developing world in the crafting of previous international regimes, such as the United Nations Convention on the Law of the Sea (UNCLOS)[38], the nuclear non-proliferation regime[39], the international regime on the peaceful uses of outer space [40] to name a few. However, in the recent past, India has often shied away from playing this global leadership role[41] in

[38]. India was one of the prominent developing countries which advocated for the establishment of a territorial sea of 12 miles and an Exclusive Economic Zone of 200 miles and a continental shelf to prevent the exploitation of resources in this zone by other sea-faring nations during the 31 negotiations. See G.M. Hiranandani, Transition to Triumph: History of the Indian Navy 1965-1975 (New Delhi, Lancer Publishers,2000),347.

[39] India's participation in the non-proliferation process is a good example of how it has utilised multilateral diplomacy to further its strategic interests and external identity, sometimes as a challenger to the existing status quo. See Vinod Kumar, A. (2014). Norm Entrepreneur, Catalyst or Challenger? India in the Nuclear Non-proliferation Narrative. *South Asian Survey*, *21*(1–2), 90–111.

[40] Vikram Sarabhai was the Vice-President and Scientific Chairman of the first UN Conference on the Peaceful Uses of Outer Space and was part of the scientific committees on the mitigation of space debris and space meterology and was very vocal about the emerging world reaping the benefits of outerspace despite being scientifically less advanced. See*(New Delhi, India: Harper Collins Publishers India, 2015) From Fishing Hamlet to Red Planet: India's Space Journey*, **edited by P. V.Manoranjan Rao**

[41] Sukumar, A (2018) ' how India lost its way in the study and use of International Law,' https://thewire.in/diplomacy/india-is-lagging-behind-in-the-study-and-use-of-international-lawhttps://hbswk.hbs.edu/archive/the-benefits-of-soft-power

the realm of cyber security and instead has sometimes taken a fragmented approach through bilateral diplomatic opportunities limited to the realm of defense, national security, and trade relations.[42]

Cyber security must be approached holistically through a cohesive national strategy that speaks to and brings together different strengths across the government and that looks at cyber security inherently as a national security and human rights issue. Such an approach needs to recognize that due to the interconnected nature of the world we live in today, robust national cyber security is dependent on and strengthened by global collaboration, information exchange, and shared understandings. **In this way, the work that MEA pioneers in global norm development through its past participation in the UN GGE, endorsement of the GCCS Conference in New Delhi in 2017, and contribution to the study group set up by MEITY to understand India's role in this process in the aftermath of the UN GGE is critical for the stability of India as a nation.**[43]

India has a wide variety of strategic interests in cyberspace, in the realm of digital trade and proliferation of the digital economy, law enforcement's access to data stored abroad, and the proliferation of India's digital economy. Promotion and uptake of these strategic interests can be facilitated by exercising 'soft-power'[44] and gaining international recognition from like minded countries and other stakeholders such as the private sector companies, civil society and academia.

Cyber security is a fundamental building block for a robust digital economy driven by emerging technologies, such as Artificial Intelligence and blockchain. A national cyber-security strategy is necessarily dependent on the compliance of other states with norms of responsible state behaviour in cyberspace due to the interconnected nature of the internet. If India does not participate in the norms formulation process, India may have to conform to a regime they had no say in crafting, as is the case with the Budapest Convention.[45] Instead, India's leadership role at the World Trade Organisation, where it has consistently advocated the interests of the global South - for instance, in the fields of

[42] Ibid

[43] Anuj Srivas, After UN Talks on Cyber Norms Collapse, India Starts Chalking Out Own Strategy, Wire, September 12, 2017, accessed July 3, 2018 at

[44] Joseph Nye Jr. (2004), " The Benefits of Soft Power"https://hbswk.hbs.edu/archive/the-benefits-of-soft-power

[45] Alexander Seger,(Executive Secretary Cybercrime Convention Committee, Council of Europe) " India and Budapest Convention: Why not?", accessed November 21 2017, at

agriculture and e-commerce can be a guiding example.[46] In doing so, it has allied with states positioned similarly on the issue, such as China, and attempted to carve out a niche for itself as a driver of the debate. [47]

Recognition as a key entrepreneur in the cyber norms formulation process: ("Norm appropriation")

In this context, the decision to vote for both resolutions at the UNGA allows India the flexibility to drive the norms formulation process in any direction it sees fit. Playing a leadership role and leaving an impression on a crucial and relevant global debate would enable India's positioning as a leading global power that attempts to incorporate the voices of all countries, civil society actors and the private sector into the norms formulation process.

By working towards bridging the divide in a manner that re-orients the present debate towards forging consensus, India would be leaving an imprint on the cyber norms debate and can use this imprint to leverage various other strategic concerns at the regional and global levels. As an analogy, the present geo-economic order was driven at the institutional and academic level by institutions in the US and Western Europe, which allows them to continue to drive discussion at these fora. [48] The rise of China and accompanying institutions has been backed up by Chinese attempts to re-orient the debate on the global economic regime-in a manner that suits its strategic interests and is compliant with its broader geopolitical vision.[49]

Playing a leading role as an advocate for issues that impact the region and other Global South countries

India now has an opportunity to carve out a unique position for itself as a voice that reflects the interests and priorities of countries in the Global South. It is imperative that the only voices shaping the cyber regime are not that of the 'cyber superpowers'[50] on either side of the divide.

[46] Jayashree Sengupta (2017), " India,China on the same side at WTO,"<https://www.orfonline.org/research/india-china-on-the-same-side-at-the-wto/>

[47] Ibid

[48] Marius Roska Nymoen (2017, "The United States Economic Hegemony"https://brage.bibsys.no/xmlui/bitstream/handle/11250/2455306/marius_roska_nymoen_master.pdf?sequence=1

[49] Anthea Roberts,Henrique Moraes and Victor Ferguson(2018), " The Geo-economic world order"<https://www.lawfareblog.com/geoeconomic-world-order>

[50] Matthew Crandall and Bradley Thayer (2018), " The Balance of Cyberpower"<https://nationalinterest.org/feature/balance-cyberpower-36637>

Recommendations

High-Level

It is important that pursuing global norms formation becomes a key component of India's larger approach to cyber security. **Such an approach should be driven both by the MEA and the MoD**, who should work towards two seperate but interlinked and cohesive documents outlining each Ministry's strategic national and global vision in cyber security for reasons that are discussed below. The Government of India (GOI) should update its National Cyber Security Strategy, 2013 to incorporate and align with both these strategies and ensure that they speak to one another seamlessly.

The prevailing standards of International Law combined with both short and long-term strategic considerations should drive a nation's approach to any international process. However, a grand strategic vision needs to bring together external and internal national considerations..[51] In this way, the Ministry of Defense plays a key role in devising a coherent 'cyber defense strategy ' that:

1. Constructs a cohesive cyber security ecosystem for India which ensures multistakeholder process and collaboration between security researchers, private sector, civilian nodal agencies and the military.
2. Charts out a cyber deterrence strategy which outlines India's approach to engaging with external cyber adversaries and enhances India's military positioning-both in the cyber and kinetic realm. This includes, laying out standards for public attribution, along with the role of various authorities in this process.[52]
3. Lays down a framework for cyber defense alliances with international partners through regular confidence building measures-such as cyber security exercises and information exchange.

There are crucial overlaps between the Cyber Strategy that should be devised by the MEA and the Cyber Defense Strategy devised by the MoD. The framework outlined in the cyber defense strategy should be firmly grounded in International Law and the norms

[51] **Grand strategy** or **high strategy** comprises the "purposeful employment of all instruments of power available to a security community See Gray, Colin: *War, Peace and International Relations: An Introduction to Strategic History*, Abingdon and New York City: Routledge 2007, p. 283.

[52] Basu, A, "Lessons from US responses to cyber attacks",https://www.thehindubusinessline.com/opinion/lessons-from-us-response-to-cyber-attacks-ep/article25372326.ece,accessed Nov 03 2018;

for responsible state behaviour in cyberspace. In turn, the MEA's leadership role in the global norms formulation process should be underscored by a strong national security and national deterrence architecture.

While the two cyber strategy documents should be in sync, they can also be viewed independently. The MEA should not constrain itself only to issues of cyber defense but should also chart out global economic, political and cultural visions of cyberspace and articulate the 'development dimension of cyber norms' as a leading voice for the Global South. On the other hand, conducting offensive or defensive operations and securing information infrastructure should come within the exclusive competence of the MoD strategy.

Specific Points of action and research for the MEA

1. Ensure that India's approach to cyber norms formulation is incorporated into the next National Cyber Security Strategy

A survey of cyber strategies across six countries-spanning across economic, military and regional diversity, reveals that at least a high-level approach to cyber norms formation has been articulated in all strategies studied. Some countries like Singapore, UK, Japan and Chile have a single cybersecurity strategy that includes a section on international cooperation. Within this section, the role of the foreign ministry and the defense ministry and other municipal authorities are clearly demarcated, such as in the Japanese strategy. **(Model 1)**

Other countries, like Australia and USA have two seperate cyber strategies-a broader one focussing on domestic cyber resilience and a more specific one focussing on external affairs. **(Model 2)**The US Department of Defense has also released a separate cyber strategy which outlines how the military will be engaging in cyber defense against external actors. More detailed coverage of these strategies has been included in Annex 2.

In order to create an effective and sustainable cyber strategy, the role each government department plays in this ecosystem needs to be clearly demarcated and avenues for cooperation across departments need to be charted out. Either of the two models may work, depending on the extent of autonomy each department desires in crafting out their role in this process.

2. Play a leadership role in global negotiations through concerted pragmatic cyber engagement at the multi-lateral, regional and bilateral level by:

- Pro-actively engaging in the UN-GGE through norm proliferation for ‘responsible state behaviour; at three levels -
    - ❖ **Technical norms:** Developing norms for technical co-operation among member states and private actors to protect information infrastructure across borders
    - ❖ **Building on International Security Norms:** India should attempt to build on the Tallinn Manual to develop effective parameters and guidelines for states that may enable them to effectively comply with standards of International Law such as the obligation of due diligence or the parameters required for effective attribution as per the Law on State Responsibility.[53] In doing so, India should advocate the application for the well-accepted International Law tenet of Common but Differentiated Responsibilities (CBDR)[54] in cyberspace. Due to the large gap in capacity across states, a core challenge faced by the norms formulation process in cyberspace lies in ensuring that all states can ‘fulfil their responsibilities’ and discharge their obligations in International Law. This question becomes particularly relevant when charting out common due diligence obligations and obligations of co-operation as recognised by the 2015 GGE Report.
    - ❖ **Articulate a development dimension of cyber norms:** A development dimension of cyber norms should be built on three fundamental tenets[55]: (a) Information infrastructure as an utility and entitlement for every citizen in terms of accessing services, (b)

[53] See Arindrajit Basu (2018), “ The Potential for the Normative Regulation of Cyberspace”<https://cis-india.org/internet-governance/files/normative-regulation-of-cyber-space-report>, 25-33

[54] The Rio Declaration,which contains a clear articulation of the CBDR in Principle 7 states that “The Rio Declaration states: “In view of the different contributions to global environmental degradation, States have common but differentiated responsibilities. The developed countries acknowledge the responsibility that they bear in the international pursuit of sustainable development in view of the pressures their societies place on the global environment and of the technologies and financial resources they command.” See Shackelford, Scott J.; Russell, Scott; and Kuehn, Andreas (2016) "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," Chicago Journal of International Law: Vol. 17: No. 1, Article 1

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

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 need adequate resources including skilling and financial resources and (d) Using ICTs for furthering socio-economic rights and civil and political rights in line with the United Nations Sustainable Development Goals 2030 and commitments made by India and other countries to the International Covenant on Civil and Political RIghts (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR).

Thus far, discourse on cyber norms has been limited to the First Committee of the United Nations General Assembly, which limits itself to Disarmament and International Security Affairs. India needs to ensure that discussion on cyber norms also extends into work being put forward by the Second Committee (Economic & Financial) and Third Committee (Social, Humanitarian & Cultural) It should be looked as a crucial tool towards meeting the United Nations Sustainable Development Goals in 2030.[56] 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.

- Commission inter-disciplinary research from academia and civil society in India and the region in order to help formulate India's position at the GGE and other international fora. These experts should come from a wide range of disciplines, including international law, technical commentary and other social science disciplines

- Take initiatives on inter-sessional meetings with various stakeholders across the globe and ensure that the feedback is filtered back into the UN driven process

[56] http://www.un.org/en/sections/issues-depth/big-data-sustainable-development/index.html

3. Articulate India’s position on how International Law applies in cyberspace

So far only the United States,[57] Germany[58] and the United Kingdom[59] have clearly charted out their position on how key tenets of International Law apply to cyberspace with justifications on why they believe this to be the correct position. Even though these positions are not universal, as was evident from the break-up of the UN-GGE, articulating these positions publicly communicates to other states the range of offensive and defensive measures a state believes it is legally valid to engage in. This can lead to behavioral convergence around expected norms as states correctly perceive strategies being deployed by other states . As stated by Brian Egan, former US Legal Advisor to the State Department, a lack of clarity from states “could rise to misperceptions and miscalculation by States, potentially leading to escalation and, in the worst case, conflict’ [60] Given the limited number of statements being put forward and the similarity in the positions thus articulated, a well-reasoned statement from India might open the gateway for non western-centric constructions of International Law, which account for the unique interests and realities of the global south countries.

4. Consider the possibility of an International Convention on Cyberspace as a beneficial tool for fostering participatory consensus among a variety of stakeholders

There is a clear divide among both academics and policy-makers on the ideal governance mechanism for responsible state behaviour in cyberspace. The USA and other western states, including the NATO allies believe that existing international law is sufficient to carve out norms of responsible behaviour and there is no need to draft a separate treaty for the purpose. On the other hand, Russia, China and its allies in the Shanghai Cooperation Organisation reject the applicability of all parameters of International Law and underscore the need for a new treaty regime.

In 2004, Raustiala & Victor coined the term “regime complex,” defining it as “an array of partially overlapping and nonhierarchical institutions [driven by various constituent

[57] https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf
[58] https://www.lawfareblog.com/germanys-position-international-law-cyberspace
[59] https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century
[60] https://www.justsecurity.org/wp-content/uploads/2016/11/Brian-J.-Egan-International-Law-and-Stability-in-Cyberspace-Berkeley-Nov-2016.pdf

elemental regimes] governing a particular issue-area." [61] Joseph Nye has argued that a regime complex through cyberspace can enable co-operation on certain issues despite disagreements in others.[62] For example, China and US can engage in economic co-operation even if they differ on information control and human rights online.[63]

While the position articulated against a treaty-driven hierarchical regime is valid, a core aspect of a regime complex is the absence of hierarchy among the elemental regimes, which effectively means that resolution of conflict is driven by actors with greater voice or influence.[64] Further,multiplicity of regimes in a specific issue area leads to fragmentation of that issue area. A direct pragmatic spill-over of this is that countries/civil society members from the Global South can attend fewer conferences due to financial and logistical constraints, and therefore have less say. Fragmentation also allows for 'Exit'-where states can exit institutions where they are numerically overpowered and can continue to craft the regime by simply joining an alternate one or creating one

Given this backdrop, India might consider galvanizing efforts towards an all-encompassing cyber convention driven by multi-stakeholder consultations and subsequently signed and ratified by all states.Ideally, an initial draft resolution calling for negotiations on a cyber convention as one of its operative clauses should be tabled at the 76th Session of the UNGA after the UN-GGE (that will be formed in 2019) submits its report. [65]

[61] Karen Alter and Karl Raustila," The Rise of International Regime Complexity" Annu. Rev. Law Soc. Sci. 2018. 14:329–49https://www.annualreviews.org/doi/pdf/10.1146/annurev-lawsocsci-101317-030830

[62]Joseph Nye. "Normative Restraints on Cyber Conflict." Paper, Henry Stewart Publications 2398-5100 (2018), vol. 1. Cyber Security: A Peer-Reviewed Journal, August 28, 2018<https://www.belfercenter.org/sites/default/files/files/publication/Nye%20Normative%20Restraints%20Final.pdf

[63] Ibid

[64]

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

ANNEX 1

Votes against and abstentions on Russian and US resolutions tabled at UNGA First Committee, 73rd Session, 2018

	L-27 (Russian Federation) (170 total votes)			**L-37 (USA) (168 total votes)**		
	Sponsors	**No**	**Abstention**	**Sponsors**	**No**	**Abstention**
1.		Albania (E)	Antigua Barbuda (Car)		Bolivia (S.A.)	Algeria (Afr)
2.		Australia (A-P)	Bahamas (Car)		China (A)	Angola (Afr)
3.		Austria (E)	Brazil (S.A.)		Cuba (S.A.)	Belarus (E)
4.		Belgium (E)	*Botswana (A)*		Dem PR of Korea (A)	*Botswana* (Afr)
5.		Bulgaria (E)	Chile (S.A.)		Egypt (M.E.)	Burundi (Afr)
6.		Canada (NA)	*Cote D'Ivoire* (A)		Iran (M.E)	Cambodia (A)
7.		Croatia (E)	*Equatorial Guinea* (A)		Nicaragua (SA)	*Cote D'Ivoire* (Afr)

8.		Cyprus (E/M.E.)	*Fiji* (A-P)		Russia (M.E.)	*Equatorial Guinea* (Afr)
9.		Czech Republic (E)	Haiti (N.A.)		Syria (M.E.)	*Fiji* (A-P)
10.		Denmark (E)	Papua New Guinea		Venezuela (S.A.)	Laos PDR (A)
11.		Estonia (E)	Rep. of Korea (A)		Zimbabwe (A)	Lebanon (M.E.)
12.		Finland (E)	Rep. of Moldova (E)			Myanmar (A)
13.		France (E)	*Senegal (A)*			Namibia (Afr)
14.		Georgia (E)	*Rwanda (A)*			Palau (A-P)
15.		Germany (E)	Switzerland (E)			Papua New Guinea
16.		Greece (E)	Turkey (A/E)			*Rwanda* (Afr)
17.		Hungary (E)				*Senegal* (Afr)
18.		Iceland (E)				Uganda (Afr)
19.		Ireland (E)				

20.		Israel (M.E.)				
21.		Italy (E)				
22.		Japan (A-P)				
23.		Latvia (E)				
24.		Liechtenstein (E)				
25.		Lithuania (E)				
26.		Luxembourg (E)				
27.		Malta (E)				
28.		Montenegro (E)				
29.		Netherlands (E)				
30.		New Zealand (A-P)				
31.		Norway (E)				
32.		Poland (E)				
33.		Portugal (E)				
34.		Monaco (E)				

35.		Slovakia (E)				
36.		Romania (E)				
37.		Slovenia (E)				
38.		Spain (E)				
39.		Sweden (E)				
40.		The FYR of Macedonia (E)				
41.		San Marino				
42.		Ukraine (E)				
43.		United States (NA)				
44.		United Kingdom (E)				
45.		Andorra (E)				

(This table was compiled with Research Assistance from Shruti Trikanad)

ANNEX 2

Singapore

Singapore has a single cybersecurity strategy released by the Prime Minister and drafted by the Cyber Security Agency (CSA)[66] It is premised on four pillars.

1. Building a Resilient Infrastructure: This looks to enhance Singapore's Critical Information Infrastructure (CII) Program and mount multi-sector cybersecurity response plans by beefing up national institutions like the National Cyber Incident Response Team (NCIRT) and the National Cyber Security Centre.

2. Creating a safer cyberspace: This pillar envisages effectively tackling cybercrime by working with various global institutions, industry and partners to reduce malicious traffic.

3. Developing a Vibrant Cybersecurity Ecosystem: This envisages developing a highly skilled IT workforce and collaborating with Institutes of Higher Learning and local start-ups to ensure adequate skilling and capacity among the population.

4.Strengthening International Partnerships: The fourth pillar focusses on co-operation with the global community, in particular ASEAN on transnational cyber-security and cyber crime issues.It call for regional and dialogue on norms formulation, although it stops short of advocating Singapore's view on the global cyber norms formulation process.

UK

The United Kingdom Cyber Strategy, 2016[67] considers responses to transnational cyber threat, as a combined effort between military action and diplomatic endeavours. The Cyber Security Operations Centre (working closely in collaboration with the civilian National Cyber Security Centre) deploying offensive and defensive cyber operations in co-ordination with NATO and other allies.

Further, in Chapter 8, it considers international co-operation in cyberspace as a foreign policy issue. It envisages action on a number of planks, including :

[66] https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf
[67] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

1. Work towards a common understanding of responsible state behaviour in cyberspace;
2. Promote agreement on the applicability of international law in cyberspace;
3. Continue to promote the agreement of voluntary, non-binding, norms of responsible state behaviour;
4. Support the development and implementation of confidence-building measures
5. Work in concert with traditional geo-political allies and new partners, including multi-stakeholder initiatives such as the 'London Process' to establish and maintain strong active political and operational relationships; creating the political conditions to build strong global alliances;
6. Use influence with multilateral organisations such as the United Nations, G20, European Union, NATO, OSCE, Council of Europe, the Commonwealth, multi-stakeholder initiatives such as the 'London Process' and within the global development community

Australia

Australia has two cyber-security strategies. The first cyber strategy released by the Executive and titled *Australia's Cyber Security Strategy* has an overview of various themes in promoting cyber-security in Australia and has a number of themes.[68] The second, *titled Australia's International Cyber Engagement Strategy* specifically outlines Australia's cyber engagement at the international level and is driven by the Department of Foreign Affairs and Trade (DFAT)[69]

Australia's has four constituent themes[70]:

1. **A national cyber partnership** that ensures that cyber-security is a multi-stakeholder initiative
2. **Strong cyber defences**, in conjunction with the military
3. **Global responsibility and influence** in supporting norms and standards for conduct in cyberspace
4. **Growth and innovation to enable Australia's private sector to make optimal use of the digital ecosystem**

[68] https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf

[69] https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf

[70] https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/PMC-Cyber-Strategy.pdf

5. **A cyber smart nation** that focuses on re-skilling professionals in order to further cyber security best practices.

Australia’s strategy for international engagement focuses on several pillars including:

1) **Digital Trade** that facilitates private sector exchanges, regulatory co-operation at the bilateral, plurilateral and multilateral levels
2) **Cyber Security at the regional and global level** through (a) Maintaining strong cyber security relationships with international partners, (b) Encourage innovative cyber security solutions and deliver world leading cyber security advice and (c) Developing regional cyber security capability Promote Australia’s cyber security industry;
3) **Cybercrime co-operation** at the global and regional level driven by (a)Raising cyber crime awareness in the Indo-Pacific;(b)Assisting Indo-Pacific countries to strengthen their cybercrime legislation; (c)Deliver cybercrime law enforcement and prosecution; (d)Capacity building in the Indo-Pacific; (e)Enhancing diplomatic dialogue and international information sharing on cybercrime;
4) **International Security and Cyberspace** to promote a stable and peaceful online environment which includes (a) Setting clear expectations for state behaviour in cyberspace, (b)Implementing practical confidence building measures to prevent conflict and (c) Deterring and responding to unacceptable behaviour in cyberspace;
5) **Internet Governance and Co-operation** to achieve an open and free internet through multi-stakeholder collaboration;
6) **Human rights and democracy online** to support efforts to protect human rights and democratic principles online at the national and global level by supporting international efforts;
7) **Technology for Development** which is a crucial pillar that looks to use digital technologies to achieve sustainable development and inclusive economic growth

Japan

The 2018 Japanese Cyber Security Strategy[71] is built on four prongs at the policy level:

1) Ensuring socio-economic vitality and sustainable development
2) Building a safe and secure society
3) Strengthening security in government bodies and government entities
4) Contribution to peace and stability of the international community and Japan’s National Security

[71] https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf

The policy clubs cyber diplomacy and cyber defense under prong four but treat each issue differently. For example Prong 4.3.2 titled ‘ Strengthening Capabilities for Defense, Deterrence, and Situational Awareness’ looks at cyber resilience and cyber deterrence strategies across various stakeholders.Prongs 4.3.1 entitled ‘Commitment to a Free and Secure Cyberspace’ and 4.3.2 ‘International Co-operation and Collaboration’ focus on norms promotion and alliance-building,which is an external affairs mandate.

Chile

The Chilean cyber security strategy has a section on international co-operation, which is driven by principles of Chilean foreign policy that include” the respect for international law; the promotion of democracy; the respect for human rights; conflict prevention; the pacific resolution of disputes and the commitment to cooperate in the international arena. In turn, these principles drive the interest of Chile’s foreign policy, namely: contribute to the strengthening of multilateralism and promote international peace and security.”[72]

The pillars of this strategy are driven by :1) Co-operation and assistance, 2)Re-enforcement of participation in multi-lateral and multi-stakeholder work and 3) Promotion of international regulations for trust and security in cyberspace

USA

In September 2018, the White House and Department of Defense released two seperate cyber strategy documents. The document released by the White House is entitled ' National Cyber Strategy for the United States of America' and articulates the four pillars on which the United States's cyber vision will rest.[73] These include : “**1) [Defense of American information infrastructure]**Defending the homeland by protecting networks, systems, functions and data, **2) [Promotion of America’s economic interests]** Promoting American prosperity by nurturing a secure, thriving digital economy and fostering strong domestic innovations, **3) [Preserving peace and security globally]** by strengthening the ability of the United States-in concert with allies and partners-to deter and if necessary, punish those who use cyber tools for malicious purposes and **4) [Playing a global leadership role]** Expand American influence abroad to extend the key tenets of an open, interoperable,reliable and secure internet.”

[72] https://ccdcoe.org/sites/default/files/documents/NCSP%20(ENG).pdf

[73] https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

The Department of Defense Cyber Strategy[74] focuses on (1) Ensuring the Joint Force can achieve its missions in a contested cyberspace environment, 2) Strengthening the Joint Force by conducting cyberspace operations that enhance U.S. military advantages, 3) Defending critical U.S. infrastructure from malicious cyber activity,4) Securing DoD information and systems against malicious cyber activity and 5) Expanding DoD cyber co-operation with interagency, industry and international partners."

[74] https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF