THE CENTRE FOR internet & society

CIS Comments on ‘Pre-Draft’ of Report of the United Nations Open Ended Working Group

April 6th,2020

By **Arindrajit Basu**
With Inputs from **Elonnai Hickok**
Reviewed and Edited by **Elonnai Hickok**

About the Centre for Internet&Society, India

The Centre for Internet and Society, India (CIS) (cis-india.org) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The academic research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

CIS would like to thank the Open Ended Working Group for making public the 'pre-draft' report of the Open Ended Working Group (OEWG). The publication of the draft is in line with the principles of transparency and openness that founded, and continue to define the OEWG process. As a research organisation, we will use this brief intervention to highlight key research areas, avenues of discourse, and next steps that both states and non-state actors involved in the OEWG should bear in mind going forward.

1. Holistic conceptions and framing of security and grounding in human rights

We firmly believe that security should be considered a positive concept-as the feeling of individuals and communities feeling secure, rather than a mere absence of harm-as defined by the state. We commend the OEWG on recognizing this human-centric lens to cyber-security. As recognised in the recent statement by the Freedom Online Coalition, human rights and security are "*complementary, independent and mutually re-enforcing*" [1] and should be seen as critical in working towards guaranteeing the availability, integrity, and accessibility of Information Communication Technologies (ICTs). **Denial of civil and political rights often enable the suppression of socio-economic rights, thus leading to a negation of security.** We strongly encourage states, private sector actors and global governance mechanisms to adopt this framing of security as deliberations move forward.

2. Threats

We welcome the discussion on the diverse range of threats to Information Communication Technologies (ICTs) that exist in the present day-both from states and non-state actors. We identify two further clusters of threats that need to be explicitly discussed:

(a) Global linkages in surveillance technology and influence of the industry

The private partners in the global surveillance industry continue to aid state suppression by providing relatively low cost access to spying tools that were only within the purchasing power of the most advanced economies. [2]A report by the UN Special Rapporteur on Freedom of Speech and Expression comprehensively documents the workings of this industry.[3]

[1]" Freedom Online Coalition Statement on Human Rights and Cyber Security,"(2nd Feb 2020)https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf

[2] " The Surveillance Industry in the World" (16th February,2018)https://privacyinternational.org/explainer/1632/global-surveillance-industry

[3] Report of the United Nations Special Rapporteur on Freedom of Opinion and Expression (25 June 2019)https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736

Through a number of techniques including computer interference, mobile device hacking, network surveillance, and facial recognition, the global surveillance industry has pervaded all forms of communication and digital existence today. Government agencies and departments have their requirements while private companies have the incentives and expertise to service those needs. Reporting by civil society and academia on the operation of this industry highlights that the engagement does not limit itself to the stage of sale. [4]Instead, the expertise of the companies continue to be used to conduct training and continue to upgrade and customise the malware to conduct the most intrusive forms of surveillance possible on their targets. Further, the surveillance industry has an overbearing influence on the trajectory of human rights and data protection policies and regulatory frameworks today.[5]

While a limited enhancement of surveillance techniques and strategies may be necessary and legally justified in clearly defined instances of national and public interest and safety, such use must be guided by the principles of necessity, proportionality, legality, and legitimacy. Without these principles, the carte blanche' use of surveillance can target dissidents working on key issues and ultimately compromise national security. **The export and import of surveillance technology deeply impacts activism on key issues that impact vulnerable communities in developed and developing countries alike. Therefore, the overbroad export, import, and use of surveillance technologies cannot be viewed solely as a threat freedom of expression and privacy but must also be considered by the OEWG as a key threat to national security and cyber security.**

(b) Denial of access to the internet and communications networks

Another key threat to global cybersecurity is the denial of access to the internet by states through means such as slowing network speed, censoring certain parts of the internet or removing content ,or shutting down the internet entirely. In today's digital age, restricting access to the internet and communication networks poses a grave risk to the safety, security, wellbeing, and livelihood of individuals. Such a risk becomes exacerbated in times of national and global crisis like we are seeing today. This further harms the local economy, stifles free speech, and enables the spread of verbal misinformation as the internet then ceases to exist as a verification mechanism. While misuse of the internet through information operations and kinetic attacks must be condemned, the internet continues to be a source of empowerment and security for many individuals across national borders-including refugees and migrants. **Therefore, accessibility to the internet must be considered as an integral security issue and the OEWG must carve out recommendations on the limited scenarios and processes by which states can deny access to the internet.**

[4]Siena Anstis, Ron Deibert, Miles Kenyon, and John Scott-Railton, " The Dangerous Effects of Unregulated Commercial Spyware" (June 24,2019) https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/

[5] Reporters Without Borders, "International regulations: broken or blocked by lobbies", 14 March 2017.

3.International Law

We welcome the discussion and recommendations of the OEWG on a consensus-driven approach to fermenting international law in cyberspace. This must be driven by states articulating their viewpoints on the issue-which will over time lead to the crystallization of customary international law. It is important that diplomatic engagement on cyber stability uses the language of international law to frame positive conflict among a cross-section of stake-holders in order to galvanize consensus in the long run.[6]

We would like to highlight two specific issues:

(a) Legally binding treaty

We recognize the need for a legally binding instrument that governs cyberspace. An international legal framework would lead to certainty and predictability through clear legal obligations which can be enforced through specialized dispute resolution fora. Second, it would allow for the breaking of the artificial barrier between the security and the development dimension of cyberspace. Finally, if negotiated with widespread consultation, it is likely that the final terms of such a legal framework will represent a far greater number of interests than the current fragmented approaches on cyber norms or countering cyber crime. Scholars have demonstrated that fragmentation of governance regimes furthers regulatory confusion and often disadvantages developing countries and civil society actors,who are able to gain more leverage through coalitions at single fora -such as the G77. [7]

It is critical, therefore, that the final treaty governing cyberspace looks beyond the narrow security dimension and is negotiated at a seperate, single convention beyond the topical confines of the United Nations First Committee. **The treaty must cover questions such as ICTs for development, the exploitative practices on data governance adopted by large multi-national companies, and the geo-politics of cross border sharing of data - while also carving out strict obligations aimed at guaranteeing security,stability and the preservation of human rights in cyberspace.**

Previous research we have undertaken highlights how previous regimes evolved through three phases-the diagnostic, formulae-setting, and details phases.[8] We highlighted how protracted discussion towards cultivating an international treaty brought out discussion on core values, strategic interests, and equity that any global governance regime must take into account. **We feel that the OEWG could kickstart a process toward an omnibus convention on cyberspace, which will enable various stakeholders to come together towards forging predictability and equity in cyberspace.**

[6] Monica Hakimi, " The Work of International Law" 1 HILJ 58 (2017) 5

[7] Eyal Benvenisti and George W.Downs," The Empire's New Clothes: Political Economy and the Fragmentation of International Law". Stanford Law Review, Vol. 60, 2007. Available at SSRN: https://ssrn.com/abstract=976930

[8] Elonnai Hickok and Arindrajit Basu, " " Conceptualizing an International Security Architecture of Cyberspace", Briefings of the Global Commission on the Stability of Cyberspace,https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf

(b) Red lines through the application of International Humanitarian Law in Cyberspace

Most cyber attacks qualify as 'below the threshold' operations that do not amount to the 'use of force' as per Article 2(4) or an 'armed attack' triggering the right of self-defense under Article 51 of the United Nations Charter- a situation described as a 'state of unpeace' in cyberspace. This makes the application of *jus ad bellum* ('right to war') inapplicable to most cyber operations.[9] However, the application of 'jus in bello' (law that governs the way in which warfare is conducted) or International Humanitarian Law (IHL) does not need armed force to be of a minimum level of intensity but guarantees protection of civilians and unnecessary suffering. **Therefore the principles of IHL that have evolved in the Geneva Conventions should mark 'red lines' that limit collateral damage as a result of cyber operations.**[10] No state should conduct cyber operations that intend to harm civilians and states should use all means at its disposal to prevent this from happening. It has been especially disheartening to see hospitals and other institutions providing healthcare during the COVID-19 crisis become victims of cyber attacks.

(c) Attribution

We welcome with appreciation the pre-draft's recognition that a universally acknowledged approach to attribution must be undertaken. Given the technical challenges in attributing cyber attacks to a state, the present standards of attribution in the law of state responsibility need to be reconsidered. In 2017, Peter Stockburger proposed a new test known as the 'control and capabilities' test which he argued could be the *lex specialis* (specific law) for determining international responsibility when attributing cyber attacks.[11] This approach moves away from the narrow focus on 'control' embodied in the traditional 'effective control' test and instead relies on multiple other indicative factors that could instead make this determination. This includes:(1)Relationship between non-state actor and state, (2) The influence the state exerts over the non-state actor; (3)Methods employed by the non-state actor; (4) Motivations of the parties involved ; (5)whether they use similar code; (6) Technical capabilities of the non-state group and (7) geographic location.[12]

We also commend the efforts of independent institutions such as the Cyber Peace Institute[13] that are seeking to close the accountability gap in cyberspace by adopting a collaborative approach to attribution. We encourage the OEWG to consider how independent institutions and existing bodies and initiatives such as the Cyber Peace

[9] "Fundamental Principles of International Humanitarian Law",https://casebook.icrc.org/glossary/fundamental-principles-ihl

[10] Veronique Christory " Cyber warfare: IHL provides an additional layer of protection" 10 Sept,2019,https://casebook.icrc.org/glossary/fundamental-principles-ihl

[11] Peter Z.Stockburger, " Control and Capabilities Test: Toward a New Lex Specialis Governing State Responsibility for Third Party Cyber Incidents" in H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.) 2017 *9th International Conference on Cyber Conflict:Defending the Core* (2017 NATO CCD COE Publications, Tallinn) 1

[12] *Ibid*

[13] Disclosure:Sunil Abraham, former Executive Director of CIS is on the Advisory Board of the Cyber Peace Institute. The Hewlett Foundation, one of the co-funders of the institute also funds CIS

Institute and the Global Commission on Stability in Cyber Space can contribute to multi-lateral efforts attempting to secure stability in cyber space.

4. Confidence Building Measures

We note with appreciation the OEWG's focus on confidence-building measures-in particular the suggestion of National Points of Contact and the focus on regional institutions. Historically, the implementation of CBMs have enabled the diffusion of norms for fostering responsible state behaviour.[14] However, the success of CBMs in non-western contexts has been less clear due to differences in the actors, institutions, and socio-economic realities.[15] Research we are undertaking looks at the specific question of how CBMs have fared in non-western contexts, and we encourage the OEWG to think about the specific conditions, vectors and pre-requisites that enable a CBM to become successful-either in promoting norms or in cultivating stability across contexts and regions. Further, there are various types of CBMs-communication, constraint, transparency, and verification[16]-all of which are relevant in different contexts, and require different frameworks for success.

Concluding Remarks

Through its ongoing and proposed research efforts, CIS will continue to build discourse around cyber norms and the deliberations of the OEWG.Please reach out with any questions or clarifications at arindrajit@cis-india.org

[14] JJ Holst 'Confidence-Building Measures: A Conceptual Framework' (1983) 25(1) Survival 2–15.

[15] Zdzislaw Lachowski, "Confidence-Building Measures" Max Planck Encyclopedia of International Law (2006)

[16] "Confidence-Building and Nuclear Risk-Reduction Measures in South Asia," *Stimson Center* (blog), June 14, 2012, https://www.stimson.org/2012/confidence-building-and-nuclear-risk-reduction-measures-south-asia/.