CENTRE FOR COMMUNICATION GOVERNANCE AT NATIONAL LAW UNIVERSITY DELHI

COMMENTS TO THE INITIAL PRE-DRAFT OF THE REPORT OF THE OEWG ON DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATIONS IN THE CONTEXT OF INTERNATIONAL SECURITY

The Centre for Communication Governance at National Law University Delhi (CCG) was established to ensure that Indian legal education establishments engage more meaningfully with information law and policy, and contribute to improved governance and policymaking. CCG, based a public law university, is the only academic research Centre in India dedicated to working on information law and policy. We seek to embed human rights and good governance within information policy through our research, which includes the role of international and domestic law in India's national security policies, with a particular focus on cybersecurity, cyber conflict, and other emerging technologies.

We are grateful to His Excellency Ambassador Lauber, Chair of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) for adopting a consultative and inclusive approach throughout the process. We thank the Chair for making the initial Pre-Draft of the Report of the OEWG (Pre-Draft) available publicly and allowing comments from across stakeholder groups. We take this as an opportunity to submit our views on the Pre-Draft through which we hope to meaningfully contribute to this important discussion.

Our section-wise comments to the Pre-Draft are provided below:

I. EXISTING AND POTENTIAL THREATS

CCG commends the Pre-Draft for not understating the threats posed to international peace and security by malicious use of technology. The Pre-Draft rightly notes that harmful ICT incidents are both increasing in frequency, precision and sophistication, with greater connectivity bringing with it unintended risks and vulnerabilities.

CCG appreciates the Pre-Draft's acknowledgement that no State is sheltered from the digital threat landscape (para 20) while also acknowledging the differentiated impact ICT threats have on particular categories of actors as well as States, (para 17) depending on their different levels of ICT security, resilience and capacity to respond to adverse incidents. We agree with the view expressed that States must shoulder individual as well as shared responsibilities to ensure peace and stability in the digital domain (para 9). CCG is hopeful that emphasis on this issue will remain in focus and guide future discussions on determining responsibility of States in cyberspace, which should envisage the scope of such common but differentiated responsibilities in cyberspace. The unique role of the private sector as well as support from civil society and academia in fulfilling these responsibilities through collaboration and cooperation also merits attention.

The Pre-Draft correctly notes concern regarding state actors providing access to advanced ICT capabilities to non-state actors and using them as proxies (para 14). In this regard, further clarification may be required on the legal status of private military and security contractors (as distinct from vendors of ICT equipment and services) for effective operationalization of the norm against using proxies, which may be treated in law as proxies by some stakeholders.

CCG shares the concern expressed regarding the militarization of the digital space expressed in the Pre-Draft (para 15). While we agree that the *use* of offensive ICT capabilities contrary to international legal obligations ought to be the focus of discussion, we do not believe that a norm that prohibits the *development* of such capabilities is the province of international legal regulation. The effects of such a prohibition would entail an undue restriction on States' ability to conduct research and development in ICT for peaceful purposes, effectively hampering not only broader technological and economic development and acquisition of expertise, but

also the means and methods to exercise their legal right of self-defence. In the longer term, this would exacerbate the digital divide between the global North and the global South, instead of mitigating it.

The Pre-Draft lay emphasis on the importance of 'transnational' or 'supranational' critical information infrastructure and the danger posed by threats to such infrastructure to security as well as economic development. (para 19) We also fully support the International Committee of the Red Cross' (ICRC) submission[1] to place emphasis on critical civilian infrastructure sectors that enable the delivery of essential services to the population in this section, particularly the health, electrical, water and sanitation facilities.

II. INTERNATIONAL LAW

The chapeau of this section accurately captures the OEWG's objectives vis-à-vis furtherance of international law in cyberspace. We share the view that in order to foster shared understanding of international law and legal concepts, it is essential to identify specific topics of international law for more in-depth discussion aimed at preserving State obligations under the UN Charter.

We appreciate and agree with the view that international law is the foundation for stability and predictability in relations between States. (para 25) In this regard, we submit that it is imperative to define and distinguish what States understand to be a 'rule' or a 'principle' of international law as distinct from 'norms' of international law and refrain from using these concepts interchangeably for greater clarity in setting standards for responsible State behaviour.

With a view to developing common understanding of how existing international law applies in cyberspace, seven nations - Australia, Estonia, France, Germany, the Netherlands, the United Kingdom, and the United States have issued comprehensive national statements on how international law applies to cyberspace. While such national statements and guidance notes (para 31) are instructive, they must not be

[1] INTERNATIONAL COMMITTEE OF THE RED CROSS, *Comments by the International Committee of the Red Cross on the Initial "Predraft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*, 1, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-icrc-on-initial-pre-draft-report-of-oewg.pdf.

taken to reflect consensus, without explicit agreement from all States, especially from the global South. CCG seeks to emphasize the importance of retaining the inclusive and representative character of the OEWG process. In order to do so, it is imperative that the silence of any sovereign State in its domestic policies on emergent norms must not be considered as acquiescence or implied consent to observe such voluntary, non-binding norms.

There is a consensus on the applicability of international law to cyberspace. We agree that efforts to address security in the use of ICT should be consistent with international law, in particular the Charter of the United Nations, and respect the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the UN Guiding Principles on Business and Human Rights, where appropriate.[2]

We agree that there is a need to develop common understanding on how international law is applicable. We welcome the pre-draft's suggestion that the International Law Commission (ILC) be requested to study national views and practice on how international law applies in the use of ICTs by States in the context of international security.[3] In order to do so, with regard to issues such as the distinction between norms, rules and principles of international law, which require expertise in (international) legal theory, a reference to the ILC for further study and clarification would be apposite. (para 68(a)) However, disagreements on issues that directly impact the political and security choices of States, such as definition of a 'cyber attack' as distinct from a 'cybersecurity incident', should be referred back for discussion among States within the OEWG framework to ensure an open, accessible and inclusive process (para 33). Such a division of responsibilities also holds the potential to catalyze the formation of a legally binding instrument (para 28), should member States arrive at a consensus on this point.

This division of responsibilities takes into account the specific characteristics of the ICT domain (para 31) and is in alignment with the institutional framework for the

[2] GLOBAL FORUM FOR CYBER EXPERTISE (GFCE), The Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building adopted at the Global Conference on Cyber Space at New Delhi, (Nov. 24, 2017).

[3] Geetha Hariharan, *A Landscape of Cyber Norms*, CENTRE FOR COMMUNICATION GOVERNANCE (2018).

peaceful settlement of disputes enshrined under the UN Charter. (para 32) The division described above is analogous to the relationship between the International Court of Justice (ICJ) and the UN Security Council. While the ICJ is best equipped to settle juridical questions between disputing States, the political and military dimensions of international disputes fall within the mandate of the Security Council.

CCG stands encouraged through the Pre-Draft's consideration of the importance of additional efforts to build capacity in the areas of international law, national legislation and policy in order for all States to participate on an equal footing in discussions on how international law applies to the use of ICT by States. (para 33) We believe it may be useful to highlight the potential for academia and civil society to play a positive role in such endeavours.[4]

Capacity building efforts among stakeholders must especially focus on sharing of technical know-how, particularly in the domain of cybersecurity, with a view to making the development of a common approach to attribution at the technical level (para 32) inclusive as well. Private efforts such as the Cyber Peace Institute's work in this regard to promote an evidence-led framework for accountability can also benefit the OEWG.[5]

CCG agrees with the Pre-Draft's recommendation to create a repository of States' views and practices in the application of international law (paras 30, 68(b)) would be helpful in furthering meaningful discussions.

III. RULES, NORMS AND PRINCIPLES FOR RESPONSIBLE STATE BEHAVIOUR

The Pre-Draft observes the view that voluntary, non-binding norms that reflect consensus among states are complementary to existing international law. (para 26 and 34). We agree that the 2010, 2013 and 2015 consensus reports of the UN GEE are important milestones in the process of progressive development of international law through international cooperation. We also appreciate that the OEWG is now

[4] GLOBAL PARTNERS DIGITAL, *Pre-draft of the OEWG's report on ICTs - Global Partners Digital Response* (2020).

[5] CYBER PEACE INSTITUTE, *Closing the accountability gap: A proposal for an evidence-led accountability framework* (2019), https://www.un.org/disarmament/wp-content/uploads/2019/12/cyberpeace-Institute-position-paper.pdf.

seeking to further build upon the progress in identifying non-binding voluntary norms for responsible State behaviour in cyberspace.

CCG supports this synergistic approach. It demonstrates that parallel norm-building processes ongoing at the international and regional levels through multilateral as well as multi-stakeholder fora, stand to benefit from each other in forging cooperative and collaborative partnerships.

In order to ensure that the OEWG process develops a framework that will encourage and incentivize compliance, CCG is of the view that the voluntary non-binding norms identified for discussion be tested on the anvil of existing international legal obligations of States. The process would be counterproductive if voluntary non-binding norms undermine existing rules and principles of international law, including especially the customary rule of the sovereign right to self-defence, the principle of sovereign equality, the principle of non-interference as well as the principles of necessity and proportionality.

For instance, the proposed norm against interference with electoral infrastructure[6] is naturally subsumed within and wholly consistent with the principle of non-intervention in internal affairs of sovereign States enshrined in the UN Charter. In contrast, a norm that prohibits the targeting of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)[7] may be incompatible with the customary international humanitarian law (IHL) principle of distinction. This is because all CERTs *ipso facto* perform defensive functions in cases of cyber incidents, breaches or attacks. Thus, they directly contribute to the overall (cyber)war-making effort of a State, and accordingly, may be treated as lawful targets for direct participation in hostilities, if customary rules of IHL were applied *mutatis mutandis* to hostilities in cyberspace.

This analysis is useful to illustrate the need for prudence in developing interpretations of how IHL applies to hostilities in cyberspace. (para 27) CCG is of

[6] THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, *Advancing Cyberstability*, 32 (Nov. 7 2019), https://cyberstability.org/wp-content/uploads/2019/11/GCSC-Final-Report-November-2019.pdf.

[7] UN GENERAL ASSEMBLY, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 13(k), A/70/174 (July 22, 2015).

the view that for the effective operationalization of a voluntary norm that prohibits targeting CERTs and CSIRTs, the prohibition of the use of CERTs for malicious international activity[8] ought to be a mandatory rule.

In the same context, we welcome the Pre-Draft's re-iteration that IHL neither encourages, nor legitimizes conflict in any domain. (para 25) The ICRC in a recent position paper had articulated its view that the international humanitarian law limits cyber operations during armed conflicts, and (military) cyber capabilities that qualify as weapons, just as it limits the use of any other weapon, means and methods of warfare in an armed conflict, whether new or old.[9] CCG is of the view that a crucial question in the analysis States' development and use of offensive cyber capabilities, or 'cyber weapons' through the lens of IHL is to determine whether the use of cyber weapons should be regulated under IHL as weapons or as methods of warfare[10]. The choice of categorization has far-reaching implications for the rights and obligations of States conducting hostile cyber operations as well as neutral third party States.

CCG also supports the ICRC's proposal,[11] echoed by Microsoft,[12] to include a new norm, that States should not conduct or knowingly support ICT activity that would harm medical services, facilities and personnel, and should take measures to protect them from harm. Life-saving services should be treated as protected entities under international law, in peacetime as well as in times of armed conflict.

---

[8] UN GENERAL ASSEMBLY, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 13(k), A/70/174 (July 22, 2015).

[9] INTERNATIONAL COMMITTEE OF THE RED CROSS, *International Humanitarian Law and Cyber Operations during Armed Conflicts (Position Paper)* (2019).

[10] Jeffrey T Biller and Michael N Schmitt, *Classification of Cyber Capabilities and Operations as Weapons, Means or Methods of Warfare*, 95 INT'L L. STUD. 179, 219 (2019). *See also* Gunjan Chawla et. Al., *Comments to the National Security Council Secretariat on the National Cyber Security Strategy 2020,* Centre for Communication Governance at National Law University Delhi, 24-25 (January 2020), https://ccgnludelhi.wordpress.com/2020/01/30/ccgs-comments-to-the-national-security-council-secretariat-on-the-national-cyber-security-strategy-2020/.

[11] INTERNATIONAL COMMITTEE OF THE RED CROSS, *Comments by the International Committee of the Red Cross on the Initial "Predraft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security*, 3.

[12] MICROSOFT, *Microsoft's Contribution to Draft Open Ended Working Group Report on Cybersecurity* 3, https://front.un-arm.org/wp-content/uploads/2020/04/microsoft-response-to-draft-oewg-report.pdf.

CCG welcomes the recognition of the responsibilities of all stakeholders in their use of ICTs (para 40) and the reaffirmation that States hold the primary responsibility for maintaining a secure, safe and trustable ICT environment (para 28). We also agree that the protection of 'supranational critical information infrastructure' is the shared responsibility of all States and that the general availability or integrity of the public core of the internet should be protected (para 38). CCG agrees that this norm, as formulated by the Global Commission on Stability in Cyberspace (GCSC), should find acceptance in the Pre-Draft.[13] Accordingly, CCG reiterates the need to recognize and enumerate the common but differentiated responsibilities of diverse stakeholders in the ICT environment, including the private sector as well as academia and civil society.

CCG agrees that it is vital to look ahead and develop understanding on how identified norms can be operationalized in cyberspace. (para 37) The private sector has a crucial role to play in the operationalization of many norms. In need of most attention is the concern to ensure integrity of the ICT supply chain and the obligation to notify users when significant vulnerabilities are identified. (para 38) Joint efforts and partnerships between diverse stakeholders are indispensable to operationalizing and sustaining capacity-building efforts. (para 40)

IV. CONFIDENCE BUILDING MEASURES

CCG notes with appreciation the Pre-Draft's comprehensive view of the importance of confidence-building measures (CBMs), which are vital to the realization of peace and stability in cyberspace.

We also note that Pre-Draft highlights various aspects affecting CBMs such as national policies or doctrines and national approaches to defining critical infrastructure. Measures such as developing guidance, training for diplomats and operational exercises at the technical level between CERTs (para 42), are especially important.

CCG particularly appreciates the recognition of regional mechanisms (para 46) in this regard. CCG agrees that regional organizations can play an important role in

[13] THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, *Advancing Cyberstability*, 30 (Nov. 7 2019).

developing CBMs and building capacity. The experience of the Asia-Pacific CERT, which regularly conducts drills and helps build expertise, is indicative.

CCG broadly agrees with the Report's conclusion and recommendations in these sections which include establishing a directory of Points of Contact, (para 44) encouraging regional mechanisms to engage in CBMs, the establishment of a global repository of CBMs (para 45) and the exchange of best practices in protecting critical information infrastructure (para 42) and the pivotal role envisaged for the private sector, civil society and academia in this regard (para 47).

V. CAPACITY BUILDING

CCG fully concurs with the Pre-Draft's observation that capacity building can play a critical function in enabling full participation of actors in the global normative framework, while also contributing to commitments such as the 2030 Sustainable Development Agenda. (para 48) We agree that it is imperative to address the systemic and transnational inequalities and digital divides (para 49) in a manner that is demand-driven, tailored to specific needs and contexts, evidence based, results-oriented and has sustainable impacts (para 52).

CCG is of the view that a framework grounded in the principle of common but differentiated responsibilities in the ICT environment would also contribute to these goals and enable reciprocity. In this regard, academia and civil society can play a central role in catalyzing and coordinating South-South and triangular cooperation to supplement the efforts of States with limited technological capacity. (para 53, 54)

Lastly, we welcome the Pre-Draft's acknowledgement of the need for specific measures to address the "gender digital divide". As the leading academic research centre working on information law and policy in India, it is a matter of pride for CCG that the majority of our staff has consistently comprised of women since our establishment in 2013. We remain committed to facilitating greater representation and meaningful participation of women in programs and discussions in the ICT-security space.

In conclusion, CCG[14] wishes to congratulate the Hon'ble Chair for the reflection of the OEWG's principles of inclusiveness, openness and transparency in this comprehensive and constructive Pre-Draft. We are thankful for the opportunity to be a part of this important discussion, and hope that the present submission and suggestions enumerated above will be utilized towards strengthening regular dialogue and exchanges through institutions, processes and fora that has been tasked with the development and evolution of an international legal framework for States' use of ICTs in the context of international security.

[14] Authored by Gunjan Chawla, Sarvjeet Singh and Sharngan Aravindakshan.