16 April 2020

To:
Ambassador Jűrg Lauber
Chair,
UN Open Ended Working Group:
Developments in the field of information and telecommunications
in the context of international security

Your Excellency,

Access Now is an international organization that defends and extends the digital rights of users at risk around the world. As part of this mission we operate a global Digital Security Helpline for users at risk to mitigate specific technical threats. We work directly with policymakers and regulators at national and international forums to ensure policy decisions are focused on users and those who are most vulnerable. We also host RightsCon, the world's leading conference on human rights in the digital age. Access Now, through its Digital Security Helpline, is a member of the Forum for Incident Response (FiRST), the leading global incident response network. We are founding members of CiviCERT, a coordinating network of help desks for civil society whose goal is to improve the incident response capabilities of its members and share information on threats that affect NGOs, journalists, and other human rights defenders around the world. We support emerging regional and community-based help desk efforts to further close the gap between those in need and mechanisms of support. We participate regularly in a range of UN activities on ICT and human rights in the digital age, and have participated in the proceedings of this Open Ended Working Group, including its September 2019 and February 2020 substantive sessions, and December 2019 information intersessional.

Our initial comments on the OEWG sessions and pre-draft text

We thank the Chair for the preparation and circulation of the pre-draft, and the uploading of inputs from delegates and other stakeholders. Our submission here builds on the earlier discussion paper we circulated to OEWG participants prior to the December intersessional, and the comments we delivered in the February 2020 substantive session. Our inputs here supplement the perspectives provided on the pre-draft report in the joint civil society letter of April 2020, to which we are a signatory.

Access Now believes that approaches to cybersecurity policy should be **user-centric, systemic, and anchored in open and pluralistic processes**. Flowing from this, we see the U.N. processes on global cybersecurity as important for establishing these norms, which is why we prepared a discussion paper for state delegates and other stakeholders. In that earlier **paper**, we recommended that OEWG participants prioritise work in the following key areas, along with other recommendations:

1. Defining the objective of international cybersecurity norms
2. Developing norms that address all objectives equally
3. Building a secure cyberspace with humans in mind

4. Ensuring OEWG discussions engage with the bottom-up, internationally distributed nature of cybersecurity

Additionally, we encouraged government representatives to the OEWG to address *inter alia* the following questions:

1. *What does the promotion of a safe and secure ICT environment mean? Should this objective include the international security among states, the national security interest of states, or the security and integrity of the ICT systems themselves? Where do the human rights of users and interests of at-risk communities fall?*
2. *What objective shall be achieved by the agreed norms? Where is it possible to identify gaps? Which objectives are not sufficiently addressed by the existing voluntary, non-binding norms?*
3. *How will these norms be implemented to adequately prevent and mitigate harms to individuals and societies? What measures might accompany these norms to facilitate action?*

We believe that the text of the pre-draft report of the OEWG helps address several of these concerns, but there is still work to be done. While the development of international law on the global cybersecurity norms can have several paths, we strongly believe that we all must move forward on what we do agree on. We cannot afford to wait.

A failure to continuously build on the efforts of the previous GGEs and the deliberations of this OEWG would place even more users at risk, and increase insecurity in the technologies and online communications mechanisms that are now part of the mainstream, everyday life of so much of the world's peoples - even as many still remain excluded by digital divides. We raised this concern at the February substantive meeting, and the subsequent further spread of COVID19 further reiterates the very real costs we risk if we fail to advance further understanding and progress of implementation on global cyber norms. As an unprecedented number of families, businesses, governments, and others rely on the global internet and ICTs to communicate, work, and access critical services during this pandemic, we have seen the increase in exploitation of vulnerabilities and attacks on ICT systems - including healthcare. Failure to advance human-centred and systemic approaches to improving global cybersecurity places us all at greater risk.

In particular, we believe the report of the OEWG requires further expansion and clarification in several of the areas where participants have shown agreement on the need to advance further cooperation and progress, as well as further effort on the prevention and mitigation of harms against individual users and vulnerable, at-risk communities. We also note that the pre-draft currently does not include the report emerging from the informal intersessional meeting of December 2019 chaired by Mr. David Koh of Singapore; we recommend that it be made part of final report of the OEWG given the wide recognition of the value of those discussions to the OEWG's mission as a whole.

We provide our initial feedback below to the specific sections of the pre-draft. We may supplement this with additional inputs as participant inputs are made available and the draft text evolves.

Section-wise comments:

Comments on 'Introduction'

We agree with the text in this section which recognises how ICTs have been a catalyst for human progress, and that the OEWG has noted the value of the successive GGEs and recognised that its objective is to help advance mutual understanding among all states. Additionally, we believe that the pre-draft correctly records the significant agreement shown by the OEWG on the importance of a "human-centric" lens and approach to discussions on ensuring global cybersecurity and responsible state behaviour. This is a significant achievement and this framing is crucial to correctly capture in the OEWG's report. We believe that this introductory section would benefit from further noting how many states and stakeholders recognised that a human-centric approach in particular required the observance of human rights and fundamental freedoms, including those pertaining to access to information, privacy, and data protection.

We welcome the several statements by states and regional groupings around protecting fundamental freedoms while creating and executing cybersecurity laws and policies - including references to the recent statement by the Joint Statement of the Freedom Online Coalition on "Human Rights Impact of Cybersecurity Laws, Practices and Policies". Our rights to expression, association, privacy and data protection are complementary to cybersecurity - and not opposed to it. The further specific observations made by states on how human-centric approaches to international law and cyber activities must respect the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights - particularly Articles 17, 19, and 22 - should be noted. This is relevant for several paragraphs in this section, but paragraph 12 in particular benefits from explicitly recognising human rights as constituting a key part of this human-centric approach.

The text of paragraph 9 does well to record the importance that many in the OEWG have laid on narrowing the gender digital-divide. We believe that this text should also note the many references made by participating delegations and other stakeholders on addressing the concerns of vulnerable communities in the OEWG, as well as calls made to increase avenues for them to be able to participate and enrich its deliberations.

We note and appreciate the focus in para 10 on recognising the three pillars of the UN's work. We believe that the report would better reflect the agreement by many stakeholders that these pillars are interdependent and mutually reinforcing.

Comments on 'Existing and Potential Threats'

We believe that it is important that this section of the report keep in mind the general approach of technology neutrality that was stressed by several OEWG participants. It is particular forms of

malicious usage of technologies by certain actors that should be the threat that the OEWG considers; the OEWG should avoid any over-broad demonisation of or moral panics around particular technologies.

We believe it would be useful for this section of the report to indicate that stakeholders are concerned about the impact that misuse of ICTs can have on human rights, especially given the only growing reliance by all on digital. The report text can more explicitly address the concerns raised by participants and stakeholders on the issue of vulnerabilities, particularly their stockpiling by governments as well as contractors, vendors, and other actors. The threat that insufficient disclosure of vulnerabilities to both users as well as technology developers and the private sector should be recognised in the report of the OEWG. The recognition of this reality is heightened by the current COVID pandemic and the increasing cyber risks posed to the global response to it due to vulnerabilities impacting systems and infrastructure connected with healthcare.

We also believe that the OEWG report should acknowledge the risks posed by insufficient protections and flawed policy, legal approaches to the security research community. Unfortunately today, far more often than they should, security researchers face challenging disclosure environments, legal uncertainty and harassment, intimidation, and even detention. Shortly after the OEWG informal intersessional, on 18 December 2019 (building on previous discussions at the 2019 UN Internet Governance Forum in Berlin), Access Now and over 30 organisations issued a statement on how the work of digital rights defenders is key in protecting and maintaining an open and safe online civic space. It is through their research we learn about the existence of vulnerabilities in systems, alerting and allowing governments and companies to find solutions that improve infrastructure and online security for the benefit of the public. Despite the relevance of responsible disclosure, some governments across the world are unfortunately persecuting researchers through legal cases or criminalising their activity – and the encryption we all depend on – through laws meant to silence and dissuade them. If, as a rule, governments punish the people with the expertise to disclose this information, then we are all at a security risk.

Additionally, we commend the recognition in this section - specifically paragraph 17 - of how the malicious use of ICTs by certain states and related actors can affect different people in different ways. Further language on the recognition of how cybersecurity harms can impact vulnerable communities and users at risk would be a useful addition to this text.

Comments on 'International law ; Rules, Norms, Principles for Responsible State Behaviour'

We commend the pre-draft text recognising that shared understandings on how international law applies to state cyber behaviour can be encouraged by increased exchanges by states. We support the call made to create a global repository of state practice in the application of international law, along with progress made in regional arrangements as well as other multi-stakeholder initiatives. We would recommend that any such repository mechanism as a UN follow-up process would be better placed to

advance increased understanding and enforcement of international law and rules, norms if a wide spectrum of stakeholders were allowed to supplement state self-reporting, providing their expertise and additional insights, technical knowledge. This would also further accountability, and truly facilitate responsible state cyber behaviour.

We believe that international humanitarian law does apply to state cyber behaviour, and that this fact should not be taken to sanction the increased use of force by cyber means. We also believe that the report text should note that further guidance on how it applies is a desired objective of the OEWG, and that such efforts would ensure there is further clarity in this area, correspondingly improving the protections of civilian populations.

We support the recognition made in paragraph 38 of the pre-draft text that several participants proposed that the existing norms could be upgraded , while ensuring that focus does not slip from the further solidification, guidance, and implementation on these existing norms. We agree that this should include focus on protecting the public core of the internet, as well as avoiding the disruption of infrastructure for political processes (including elections), or that which harms medical facilities (even more relevant given the COVID pandemic).

We also draw attention to the growing international stakeholder belief, including statements elsewhere in the UN system, that steps should be taken to protect against internet shutdowns and similar disruptions.

Additionally, we believe that the OEWG report should look at the protection and promotion of the security research community as an area complementary to existing global cyber norms, particularly the voluntary norm on “responsible reporting of ICT vulnerabilities,” as recommended in the UN GGE Report 2015 (A/70/174). As noted previously, security researchers face challenging disclosure environments, legal uncertainty and harassment, intimidation, and even detention. Guidance should also be provided on how governments can adopt and encourage transparent processes for the responsible disclosure of vulnerabilities that independent security researchers discover — both to private companies as well as public entities — and reform laws that conflate research activity with criminal acts. The entire internet ecosystem stands to benefit if we create incentives for, rather than punish, security research. Governments should encourage private and public entities to adopt coordinated disclosure policies (and similar best practices) and consider updating legal frameworks to reflect the nuances of intention and scope against the powers given to prosecutors when dealing with security researchers. Governments should also introduce a transparent process for how they handle and disclose vulnerabilities encountered and/or used by their law enforcement and intelligence agencies, building on the growing international recognition of the importance of vulnerability equities process, including in the recommendations of the Global Commission on the Stability of Cyberspace.

Comments on 'Confidence building measures'

We agree that the creation and operation of the OEWG does itself constitute an important CBM, as stated in paragraph 43. We believe however that effective participation of all stakeholders - including civil society, security researchers, and the wider technical community - would be critical in order for the OEWG to truly act as an effective CBM. The exclusion of effective participation and discussion with these communities in the OEWG's proceedings so far undermines its effectiveness as a CBM in itself. Additionally, the report should note the several interventions made by states and stakeholders that ensuring multi-stakeholder discussion and open processes with wide input was crucial to building confidence more generally in this area.

We recommend that the report should note the value of further discussions and initiatives amongst states and other stakeholders on responsible reporting of ICT vulnerabilities, coordinated vulnerabilities disclosure, and increased agreement around vulnerability equities processes as an important CBM.

Comments on 'Regular institutional dialogue'

We support initiatives calling for the renewal or fresh creation of the OEWG. We believe that would only be effective however if it allowed wider stakeholder engagement. Additionally, we believe that any gap between the existence of such a fora for discussion should be minimised, particularly given that the mandate currently is due to end in the 75th session of the UN General Assembly, and the current pre-draft text only proposes a potential new mandate for the OEWG in the 76th session.

We look forward to further OEWG deliberations, building on the progress shown by the meetings so far over the last few months. We hope out inputs have been of assistance to the Chair and OEWG participants, and shall continue engaging to further this important initiative.

Access Now (https://www.accessnow.org) defends and extends the digital rights of users at risk around the world. By combining direct technical support, comprehensive policy engagement, global advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For More Information, please contact:
Raman Jit Singh Chima | Senior International Counsel ; Global Cybersecurity Lead