12 February 2020

Chair,

Thank you for this opportunity to speak, and for the efforts you have led on driving forward this important OEWG in a constructive manner. We also in particular appreciate the working papers that were made available online and the questions you framed for participants.

As some of you may know, Access Now is an international non-profit organisation that seeks to defend and advance human rights in the digital age, and have our origins in providing digital security assistance to users at risk.

We fully associate with the joint civil society statement organized by Association for Progressive Communications, which is being delivered shortly afterwards; a statement to which we are also a signatory. We use this opportunity to provide additional inputs to the participants of this OEWG.

We thank David Koh from Singapore and his colleagues for their able work on organising the December informal intersessional, and for following up to ensure that the discussions there have enriched this OEWG. As we mentioned in December, and made available in our discussion paper submitted to the OEWG, there are important questions that this OEWG must use to guide its work. We believe that the discussions over the December informal intersessional and this February session have helped advance further consensus and understanding between states as well as with other stakeholders. It is our view that global cybersecurity discussions must be user-centric (or as many have put it eloquently at this OEWG - human centric), systemic, and anchored in plural, democratic processes.

As was said yesterday, there may be points that stakeholders here disagree on - but on nearly 80 percent of issues, we actually are in agreement. 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.

In short, 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 have previously stated that the OEWG would benefit if its subsequent meetings and report focused on institutionalising procedures and structures to share information and update on their national approaches to current international law governing state behaviour in cyberspace, and the additional measures and voluntary commitments taken by them. In that respect, we welcome the proposal put forward by Mexico and echoed by many states for there to be a mechanism of a repository, with periodic reporting by states. We believe a reporting mechanism with a potential stakeholder input process, which the joint civil society statement will further expand on, would be immensely valuable. We also agree with the concern articulated by Bangladesh and other states, that developing nations will require assistance with resources and capacity building to make such a repository and review process effective, and recommend that the OEWG's report also address the potential approaches to capacity building support in that regard.

We agree with the position articulated by the ICRC and mirrored by several states that international humanitarian law does indeed apply online. Recognition of international humanitarian law does not - and should not be allowed to - justify the militarisation of cyberspace and an expansion in offensive cyber operations, government hacking, and other state behaviour harming international peace and fundamental freedoms. We also agree that further development of guidance on how international humanitarian law applies and how it can be better enforced should be an objective for the OEWG to include in its report. We also stress that is is important to note that human rights defenders also greatly rely on international humanitarian law; a failure to respect and further cement the application of international humanitarian law to cyberspace and cyber operations jeopardizes the fundamental rights protected under the Universal Declaration of Human Rights, the ICCPR, and other instruments of international law.

We also support the suggestion made by South Africa that states seek to voluntarily standardise references to international law and global cyber norms in how they publish and explain attribution.

We also welcome the several statements by states and regional groupings - including references to the recent statement by the Freedom Online Coalition - around protecting fundamental freedoms while creating and executing cybersecurity laws and policies. Our rights to expression, association, privacy and data protection are complementary to cybersecurity - and not opposed to it.

We also note with the discussions around the OEWG providing guidance regarding - and the value of states affirming their support for - the additional norms that have built on the GGE norms. In particular, those of the Global Commission for the Stability of Cyberspace, and especially the public core norm, a standard to protect against internet shutdowns and similar disruptions. In the December meeting, there was also discussion around the GGE norm concerning the protection of CERTs. There has been less discussion at this meeting, though several state delegations have notably consisted of members of national CERTs.

We believe in addition to indicating the interest by stakeholders in this norm on CERTS, the OEWG report should look at the protection and promotion of the security research community as an area complementary to existing global cyber norms. Unfortunately today, far more often than it 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 and 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, many governments across the world are persecuting researchers through legal cases or criminalizing 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. Governments must come together with industry and civil society to devise solutions befitting the scale of our connected world and economies. This must include transparent processes for the responsible disclosure of vulnerabilities independent security researchers discover — both to private companies as well as public entities — and it is high time we do away with 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.

The OEWG report should also note the importance of handling vulnerabilities responsibly. 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.

We look forward to the subsequent discussions of the OEWG and the preparation of the report. We hope that the space for civil society, the technical community and other stakeholders to assist the OEWG is expanded. And we remind all its participants to focus on building on the agreements and productive discussions witnessed this week, and to take urgent steps to improve global cybersecurity and safeguard users at risk.

Raman Jit Singh Chima
Senior International Counsel
**Access Now**